C 73/4

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice / *Issues and Practices*

Computer Crime: Criminal Justice Resource Manual

Second Edition

READEX MICRO best copy available

J28.23:

About the National Institute of Justice

The National Institute of Justice is a research branch of the U.S. Department of Justice. The Institute's mission is to develop knowledge about crime, its causes and control. Priority is given to policy-relevant research that can yield approaches and information that State and local agencies can use in preventing and reducing crime. The decisions made by criminal justice practitioners and policymakers affect millions of citizens, and crime affects almost all our public institutions and the private sector as well. Targeting resources, assuring their effective allocation, and developing new means of cooperation between the public and private sector are some of the emerging issues in law enforcement and criminal justice that research can help illuminate.

Carrying out the mandate assigned by Congress in the Justice Assistance Act of 1984, the National Institute of Justice:

- Sponsors research and development to improve and strengthen the criminal justice system and related civil aspects, with a balanced program of basic and applied research.
- Evaluates the effectiveness of justice improvement programs and identifies programs that promise to be successful if continued or repeated.
- Tests and demonstrates new and improved approaches to strengthen the justice system, and recommends actions that can be taken by Federal, State, and local governments and private organizations and individuals to achieve this goal.
- Disseminates information from research, demonstrations, evaluations, and special programs to Federal, State, and local governments, and serves as an international clearinghouse of justice information.
- Trains criminal justice practitioners in research and evaluation findings, and assists practitioners and researchers through fellowships and special seminars.

Authority for administering the Institute and awarding grants, contracts, and cooperative agreements is vested in the NIJ Director. In establishing its research agenda, the Institute is guided by the priorities of the Attorney General and the needs of the criminal justice field. The Institute actively solicits the views of police, courts, and corrections practitioners as well as the private sector to identify the most critical problems and to plan research that can help solve them.

James K. Stewart
Director

U.S. Department of Justice
National Institute of Justice
Office of Justice Programs

COMPUTER CRIME

Criminal Justice Resource Manual

by

Donn B. Parker

report contributors

David C. Smith
Geoffrey W. Turner
Dr. Sanford Sherizan

August 1989

Issues and Practices in Criminal Justice is a publication series of the National Institute of Justice. Designed for the criminal justice professional, each *Issues and Practices* report presents the program options and management issues in a topic area, based on a review of research and evaluation findings, operational experience, and expert opinion in the subject. The intent is to provide criminal justice managers and administrators with the information to make informed choices in planning, implementing and improving programs and practice.

This document was prepared by SRI International under contract to Abt Associates for the National Institute of Justice, U.S. Department of Justice, contract # OJP-86-C-002. Points of view and opinions stated herein are those of the authors and do not necessarily represent the official position or policies of Abt Associates, the U.S. Department of Justice, or SRI International.

The U.S. Department of Justice authorizes any person to reproduce, publish, translate, or otherwise use all or any part of the copyrighted material in this publication, with the exception of those items indicating that they are copyrighted by or reprinted by permission of any source other than SRI International. © Copyright 1988 by SRI International.

National Institute of Justice

James K. Stewart

Director

Program Monitor

Jonathan Budd

National Institute of Justice

Washington, D.C.

The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program Offices and Bureaus: National Institute of Justice, Bureau of Justice Statistics, Bureau of Justice Assistance, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.

Foreword

With the virtual explosion of technological advances in the 1980's, computers and their applications have become an integral and indispensible part of our society and its institutions. Computers were found in one home in a hundred at the beginning of the decade – by 1987 one in five households had them. Today they are as common a business tool as the ledger or the cash register. Given this dramatic increase in the use and accessibility of computers in the home and in business, it is not surprising to see an increase in the use of computers in the commission of crime.

Law enforcement faces new challenges as it seeks to strengthen capabilities for successfully investigating and prosecuting computer crime into the 1990's. Use of computers has proliferated not only in traditional crimes of theft such as embezzlement and fraud; increasingly, drug rings, prostitution rings, child pornographers and pedophiles have turned to computers to facilitate their illicit operations just as legitimate businesses do. Police say they arrive at the scene of these criminal networks and discover computers in operation.

Detectives and prosecutors realize that if law enforcement is to make greater inroads in investigating and prosecuting these types of cases, they need to become conversant with computer operations. In fact, the 1986 National Assessment Program Survey conducted by the National Institute of Justice found that 65 percent of the police chiefs and sheriffs sampled considered approaches for handling computer crime to be a high priority for further research and information sharing.

As part of its response to this need, the National Institute of Justice has published this resource manual for the criminal justice system. An earlier edition produced by the Bureau of Justice Statistics proved to be an invaluable resource for criminal justice. This edition reflects the tremendous technological advances and statutory changes of the past decade. It is intended as a training and reference guide for investigators and prosecutors – and should prove useful to those who have limited knowledge of computers as well as to those who are familiar with computer operations.

Two companion volumes, *Organizing for Computer Crime Investigation and Prosecution* and *Dedicated Computer Crime Units*, are other important parts of NIJ's effort to provide resources to law enforcement so they can meet the challenges posed by computer crime. These reports show how state and local jurisdications have responded to confront the growing problem of computer-related crime.

The proud history of law enforcement in the United States has been marked by a remarkable capacity to successfully confront and overcome new challenges. With the publication of these volumes, the National Institute of Justice hopes to assist law enforcement and prosecutorial efforts to meet the challenges they face combating crime in the computer age.

James K. Stewart
Director

TABLE OF CONTENTS

Page

FOREWORD iii

LIST OF FIGURES ix

LIST OF TABLES ix

PREFACE xi

GLOSSARY OF TECHNICAL TERMS xiii

I. Classifying the Crime 1
- A. The Nature of Computer Crime 2
- B. Definition of Computer Crime 3
- C. Classification of Computer Crime 5
- D. History of Computer Crime 6
- E. News Media Reporting of Computer Vulnerabilities 6
- F. Investigation and Prosecution Experience 7
- G. White Collar Crime and Computer Crime 7
  1. Defining White Collar Crime 7
  2. Comparing White Collar Crime and Computer Crime 8
  3. Computer Crime Characteristics Unique from Other White Collar Crimes 8
  4. White Collar Crime Statistics 9

II. Computer Abuse Methods and Detection 9
- A. Eavesdropping and Spying 10
- B. Scanning 10
- C. Masquerading 11
- D. Piggybacking and Tailgating 12
- E. False Data Entry (Data Diddling) 13
- F. Superzapping 14
- G. Scavenging and Reuse 15
- H. Trojan Horses 16
- I. Computer Viruses 18
- J. Salami Techniques 20
- K. Trap Doors 21
- L. Logic Bombs 22
- M. Asynchronous Attacks 23
- N. Data Leakage 23
- O. Computer Program Piracy 24
- P. Computer and Computer Components Larceny 25
- Q. Use of Computers for Criminal Enterprise 27

III. Experts and Suspects 27
- A. Technical Assistance 28
  1. Electronics and Programming Experts and Witnesses 28
  2. Systems Analysts 29
  3. Computer Scientists 29
  4. Computer and Network Operators 29
  5. Data Entry Personnel 30
  6. Mainframe Computer Users 30
  7. Personal Computer Users 31
  8. Information Systems Users and Developers 31
  9. Computer-Related Organizations 32
  10. Information and Computer Security Specialists 33
  11. Auditors 33

Page

B. Characterizing Suspects 36
1. Suspects' Characteristics and Circumstances Based on Experience 38
2. Antagonistic Personnel and Organization Relationships 40
3. Interviewing Suspects 40

IV. The Computer Crime Environment 43
A. Today's Usage of Computers 43
1. Computer Usage in Science and Engineering 43
2. Computer Usage in Organizations 43
B. The Information Systems Organization 45
1. Computer Application Systems Development 45
2. Computer Operations 47
C. Physical Facilities for Computers 51
1. Protection Facilities 52
2. Technical Computer Safeguards 52
3. Operation and Production Areas 53
4. Mechanical and Electrical Support Facilities 54
5. Other Areas Related to the Data Center 54
D. The Impact of Data Communications 55
1. Computer Usage 55
2. The Information Systems Organization 56
3. Physical Facilities 56
4. Future Considerations 57
E. Computer System Vulnerabilities 57
1. Functional Vulnerabilities 57
2. Functional Locations of Vulnerabilities 59
3. Accidental and Intentional Losses 59
4. Vulnerabilities from Natural Forces 60

V. Computer Crime Prosecution 63
A. Legal Definitions in Computer Technology 63
1. Definitions of Computers 64
2. Definitions of Computer Programs 65
B. Computer Evidence Considerations 66
1. Search and Seizure 66
2. Obtaining Evidence 66
3. Personal Computer Crime Investigation 68
4. Computer Reports as Evidence 68
5. Caring for Evidence 72
6. Privacy and Secrecy of Evidence 73
7. Conjectural Forensics 73
C. Prosecution 74
1. Foundational Problems 74
2. Proprietary Rights of Computer Programs 75
3. Evidentiary Problems with Computer Records 76
4. Practical Recommendations 79

VI. Computer Crime Law 83
A. State Penal Laws 83
1. Legislative Response to Computer Crime 83
2. Technical Definitions in State Computer Crime Laws 84
3. Penalties in State Computer Crime Laws 85
4. Prosecutorial Experience with State Computer Crime Laws 86
5. Timeliness of the Law 86
6. Computer Crime Laws of Selected States 86

Page

B. Other State Authority Bearing on Computer Crime 91
1. Automatic Banking Device 91
2. Credit Card Crime 91
3. Theft by Deceit 92
4. Forgery 92
5. Obliteration or Bugging of Programs 93
6. Misappropriation of Programs 94
7. Trade Secrets 95
8. Privacy Invasions 96
C. Federal Penal Laws 96
1. Computer Fraud and Abuse Act of 1986 96
2. Electronic Communications Privacy Act of 1986 97
3. The Credit Card Fraud Act of 1984 99
4. Federal Copyright Act of 1976 100
5. Wire Fraud Act 100
6. Other Federal Authority Bearing on Computer Crime 101
7. Federal Criminal Code Provisions 102

VII. Overview of Computer and Communications Technology 111
A. Essential Elements of a Computer 111
1. Data 112
2. Programs 115
3. Programming Languages 119
B. Computer System Structure 121
1. Computing Equipment 121
2. Operating Systems 122
3. Batch Data Processing 124
4. On-line Data Processing 126
5. Process Control Systems 129
C. Data Communications and Teleprocessing 130
1. Communications Concepts 130
2. Communications Carriers 132
3. Teleprocessing 132
4. Local Area Networks 134
D. Computer Security 134
1. Access Control Software 134
2. Encryption 135

REFERENCES 137

APPENDICES
A. SELECTED STATE AND FEDERAL COMPUTER CRIME STATUTES 141
Florida 141
Colorado 143
Arizona 143
Texas 144
California 145
Federal Chapter XXI 148
Federal Chapter XVI 150

B. CITATIONS OF STATE COMPUTER CRIME STATUTES 155

C. SELECTED CASES REPORTED IN THE NEWS MEDIA 161
Introduction 161
Case Descriptions 161

Page

D. DATA PROCESSING OCCUPATIONS AND THEIR RISKS IN COMPUTER TECHNOLOGY 173
User Transaction and Data Entry Operator 173
Computer Operator 173
Peripheral Equipment Operator 174
Job Setup Clerk 174
Data Entry and Update Clerk 174
Media Librarian 175
Systems Programmer 175
Application Programmer 175
Terminal-Engineer 176
Computer Systems Engineer 176
Communication Engineer and Technical Specialist 176
Facilities Engineer 177
Operations Manager 177
Data Base Administrator 177
Programming Manager 178
Information Security Officer 178
EDP Auditor 178

E. AUDIT TOOLS AND TECHNIQUES 181
Test Data Method 181
Base-Case System Evaluation 181
Integrated Test Facility 181
Parallel Simulation 181
Transaction Selection 181
Embedded Audit Data Collection 182
Extended Records 182
Generalized Audit Computer Programs 182
Snapshot 183
Tracing 183
Mapping 183
Control Flowcharting 184
Job Accounting Data Analysis 184
System Acceptance and Control Group 184
Code Comparison 184

F. COMPUTER INTRUSION CONTINGENCY AND RECOVERY GUIDELINES 187

G. ADVANCE PREPARATIONS AND THE ACTUAL SEARCH 193

H. TIME-SHARING USAGE EXAMPLES 199

I. DIRECTORIES AND DATABASES FOR CONTACTING EXPERT WITNESSES 213

INDEX 215

LIST OF FIGURES

		Page
Figure 1	Classes of Computer Abuse	4
Figure 2	Production Process for Computer Reports	69
Figure 3	Data Flow	112
Figure 4	Data Hierarchy	114
Figure 5	A Computer Instruction	117
Figure 6	Data Stored on Magnetic Tape	122

LIST OF TABLES

		Page
Table 1	Detection of Eavesdropping	10
Table 2	Detection of Masquerading	11
Table 3	Detection of Piggybacking and Tailgating	12
Table 4	Detection of False Data Entry	13
Table 5	Detection of Superzapping	14
Table 6	Detection of Scavenging Crimes	15
Table 7	Detection of Trojan Horse Crimes	16
Table 8	Example of Rounded Down Accounts	18
Table 9	Example of Rounded Down Accounts Converted to Programmer's Account	19
Table 10	Detection of Salami Techniques	20
Table 11	Detection of Trap Door Crimes	21
Table 12	Detection of Logic Bombs	22
Table 13	Detection of Asynchronous Attacks	22
Table 14	Detection of Crimes from Data Leakage	23
Table 15	Detection of Computer Program Piracy	24
Table 16	Detection of Simulation and Modeling Techniques	25
Table 17	Occupational Vulnerability Analysis	37
Table 18	Relationship of Perpetrators' Occupations to Likely Victim	39
Table 19	Potential Antagonistic Relationships Among Different Workers in Data Processing Functions	41
Table 20	Natural Forces Causing Losses	60
Table 21	Makeup of Customer Data Record	115
Table 22	Example of Simplified Payroll Files	125
Table H-1	Time Sharing Listing: Example 1	199
Table H-2	Time Sharing Listing: Example 2	203
Table H-3	Time Sharing Listing: Example 3	207

PREFACE

The original *Criminal Justice Resource Manual on Computer Crime* was written at SRI International by Donn B. Parker and Susan Nycum in 1979 for the U.S. Department of Justice, Bureau of Justice Statistics. This revision of the manual reflects the extensive technical and statutory changes as well as computer crime loss experience that have occurred over the last 10 years. In that time, computer crime has become a mature subject of interest to a criminal justice community that must cope with 48 state and two federal statutes defining computer crime offenses.

The manual is written as both a training and reference guide for prosecutors and investigators who know only a little about computer technology as well as those with extensive technical knowledge. For lay persons, this manual provides guidelines for determining when technical and criminal justice expertise should be used and how to interact with the people who provide it. Investigators or prosecutors experienced in computer technology will find much information that will assist them in dealing with even the most sophisticated of computer crimes. Overall, then, the manual presents a simple, straightforward means of successfully prosecuting suspected computer crime perpetrators and the associated technical context.

This new version of the manual preserves the approach of assuming that readers are already experienced in traditional investigative and prosecutorial techniques. In addition, some knowledge about and experience with microcomputers is assumed. The manual concentrates on dealing with the more significant crimes associated with mainframe computer systems, facilities, and related telecommunication systems.

To take full advantage of the manual, the computer technology novice should begin by studying the overview of technology in Section VII, and by reviewing the glossary of terms. The glossary can be useful for all readers encountering unfamiliar technical terms in the text. The glossary was derived from commonly used definitions and from legal definitions in computer crime laws and legislative bills. A cross-reference index has also been included to assist readers in locating a specific subject.

The first five sections of the manual follow the typical order of events for prosecutors and investigators in handling a criminal case. Each section starts with a description of the content of that section, how it may be used, and its relevance. Those searching for more detailed information on prosecution and laws applicable to computer crime should examine Sections V and VI. Section VI was written by an attorney for attorneys and provides legal citations.

Appendixes A and B include representative computer crime laws and citations of computer crime statutes. Because some of this material will become out of date as computer crime experience increases and legislation changes, the reader should contact the state legislature of interest to ensure that the most recent statute is referenced. Appendixes C through H supply backup information for subjects referenced in the text, and Appendix I contains sources of further information and contacts.

In summary, this manual is an advanced training and reference document designed specifically to aid investigators and prosecutors in dealing with the complexity and comprehensiveness of computer crime. Much new literature followed the publication of the first version of this manual. As computer technology became a significant focus for business-related and white-collar crime, the criminal justice community responded with new capabilities and experts. This document summarizes the latest information in a form useful for prosecutors, investigators, and security specialists charged with protecting society from criminal loss.

Two companion reports funded by the National Institute of Justice are recommended as supplements to this manual. "Organizing for Computer Crime Investigation and Prosecution," by Catherine H. Conly, National Institute of Justice, Washington, DC (1989) provides information on how local jurisdictions without specialized units respond to computer crime. "Dedicated Computer Crime Units" by J. Thomas McEwen, et al., National Institute of Justice, Washington, DC (1989) reports on how several jurisdictions with specialized units have approached their computer crime problems.

GLOSSARY OF TECHNICAL TERMS

This glossary provides the contemporary meanings of the specialized data processing terms used in this manual. The glossary may be used as an independent source of information to clarify terms encountered both in investigation and in court. Where useful, the definitions have been extracted from other recognized glossaries and computer crime legislation.

The entries are arranged in alphabetical order; special characters and spaces between words are ignored. Acronyms are placed in the same sequence as other terms, according to their spelling. When two or more terms have the same meaning, definitions are given only under the preferred term. Other relationships between terms are set forth at the end of the definition, as are cross references.

ADA: A programming language developed by the Department of Defense for use in military systems and named after the first woman programmer, Ada Augusta Lovelace.

ADP: Automatic data processing.

ANI: Automatic number identification equipment used to identify calling numbers from a local exchange.

See: PEN REGISTER.

APPLICATION PROGRAM: A computer program, written for or by computer users, that causes a computer system to satisfy specific needs.

APPLICATIONS PROGRAMMER: One who designs, develops, debugs, installs, maintains, and documents application programs.

ARTIFICIAL INTELLIGENCE: The automation of human reasoning and senses.

ASSEMBLER: A computer program that translates computer program instructions written in assembly language into machine language.

ASSEMBLY LANGUAGE: A source language that includes symbolic machine language statements.

ASYNCHRONOUS ATTACK: Taking advantage of an operating system characteristic that allows dynamic rendering of functions performed.

ATM (Automatic Teller Machine): A device provided by banks for depositing and withdrawing money.

AUDIT TRAIL: A sequential record of system activities that enables auditors to reconstruct, review, and examine the sequence of states and activities surrounding each event in one or more related transactions from inception to output of final results or from final results back to inception.

AUTO DIALER: A modem or device capable of automatically generating dialed digits for a telephone call.

BACKUP: Procedure, system, or data collection to provide replication of lost files or systems in the event of a computer failure.

BASIC (Beginners All-Purpose Symbolic Instruction Code): An algebra-like computer programming language used for problem-solving by engineers, scientists, and others who may not be professional programmers. Designers of the language intended that it should be a simplified derivative of FORTRAN.

BATCH PROCESSING: The computer processing of accumulated data or of jobs accumulated in advance so that each accumulation thus formed is processed in the same computer run.

BIT (BInary digiT): In the binary (i.e., base 2) numeration system, either of the digits 0 or 1; an element of data that takes either of two states or values.

BOOT, BOOTSTRAP: To bring into a state of readiness an inactive computer; a short program designed to initiate longer programs that bring a computer into a state of readiness.

BOXING: Use of multifrequency tone generators (blue boxes) to engage in telephone toll fraud.

BULLETIN BOARD SYSTEM (BBS): A computer accessible by telephone used like a bulletin board to leave messages for other users to see.

BYTE: A sequence of usually 6 or 8 bits, operated on as a unit and often part of a computer word. This sequence may represent a character.

C: A highly efficient programming language designed to be used on microcomputers.

CAD/CAM (Computer Aided Design/Computer Aided Manufacturing): The technology involved in the automation of engineering and manufacturing operations.

CALL FORWARDING: A telephone service to forward calls to another telephone.

CASE (Computer Aided Systems Engineering): A technology supporting powerful high-level languages and tools to create sequencing, selection, and iteration instructions; acts independently of a particular underlying machine.

CHECKPOINT: A point in time or processing sequence in a computer run at which processing is momentarily

halted to record the condition of all the variables of the run, such as the position of input and output (I/O) tapes and the contents of working storage so that a failed computer run can be restarted at the intermediate point. This process, in conjunction with a restart routine, minimizes reprocessing time occasioned by computer or other failures; sometimes called callback/recovery.

CHECK SUM: A summation of bits representing the characters or numbers of a program or data file according to an arbitrary set of rules, usually used to help assure that the program or file has not been changed.

See: HASH TOTAL

COBOL (Common Business-Oriented Language): A high-level computer programming language designed for business data processing.

COM (Computer Output Microfilm): Microfilm that contains data that are received directly from computer-generated signals.

COMMUNICATIONS ENGINEER/OPERATOR: One who operates communications equipment including concentrators, multiplexors, modems, and line switching units. Ordinarily, this person reconfigures the communications network when failures or overloads occur.

COMPILER: A computer program used to translate another computer program expressed in a problem-oriented language (source code) into machine language (object code).

COMPUTATION BOUND: The state of execution of a computer program in which the computer time for execution is determined by computation activity rather than I/O activity.

Contrast with: I/O BOUND.

COMPUTER: An internally programmed, automatic device that performs data processing.

COMPUTER ABUSE: Any incident without color of right associated with computer technology in which a victim suffered or could have suffered loss and/or a perpetrator by intention made or could have made gain.

COMPUTER CRIME: Violation of a computer crime statute.

COMPUTER NETWORK: A set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

COMPUTER OPERATOR: A person who operates a computer, whose duties include monitoring system activities, coordinating tasks, and operating equipment.

COMPUTER PROGRAM: An ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

COMPUTER-RELATED CRIME: Any illegal act for which knowledge of computer technology is involved for its investigation, perpetration or prosecution.

COMPUTER SECURITY SPECIALIST: A person who evaluates, plans, implements, operates, and maintains physical, operational, procedural, personnel, and technical safeguards and controls that are related to the use of computer systems.

COMPUTER SYSTEM: A set of related, connected or unconnected computer equipment, devices, or computer software.

COMPUSEC: Computer security.

COMSEC: Communications security.

CPU (Central Processing Unit): The device in a computer system that includes the circuits controlling and executing instructions. The term may also refer to the portion of the computer that contains its electronic control, logic, and sometimes internal storage mechanisms.

CRACKER: A person who engages in computer and telecommunications intrusion.

CRT (Cathode Ray Tube) (also part of a VDT: Video Display Terminal): A device that presents data or graphics in visual form by means of controlled electron beams impinging on the face of a vacuum tube. This electronic vacuum tube is much like a television picture tube.

DATA: A representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by humans or automatic means.

See: INFORMATION.

DATA BASE: An organized collection of data processed and stored in a computer system.

DATA BASE ADMINISTRATOR: An individual with an overview of one or more data bases who controls their design and use. Responsibilities are the addition, modification, and deletion of records and frequently the security of the data base.

DATA COMMUNICATION: The transmission, reception, and validation of data.

DATA DIDDLING: The unauthorized changing of data before or during their input to a computer system. Examples are forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements.

DATA ENTRY AND UPDATE CLERK: A person who adds, changes, and deletes records in computer-stored data bases using a computer terminal or who manually updates punch cards or entries on input data forms for computer input.

DATA LEAKAGE: Unauthorized, covert removal or obtaining of copies of data from a computer system.

DATA SET (IBM terminology for a data file): Combinations or aggregations of data elements; an electronic device that provides an interface for the transmission of data to remote stations.

DATA SWITCH: A device that receives data from one or more data communication lines and communicates them to other data communication lines under program control.

DBMS (Data Base Management System): A computer application program or set of programs that provides storage, retrieval, updating, management, and maintenance of one or more data bases.

DDA (Deputy District Attorney): An attorney in the office of a district attorney.

DEBUG: To detect, locate, and remove mistakes or malfunctions from a computer program or computer system.

DECENTRALIZED PROCESSING: Data processing performed in computers that are located throughout an organization.

DEMON PROGRAM: A computer program that acts on behalf of a user (e.g., automatic searching programs).

DES (Data Encryption Standard): A standard method of encrypting data supported by the U.S. Department of Commerce, National Institute of Standards and Technology.

DESKTOP PUBLISHING: Producing high-quality printed documents using a personal computer and small printer.

DIRECT ACCESS: A method for the retrieval or storage of data, by reference to their addressable location in a storage device rather than to their location by position in a sequence.

Contrast with: SEQUENTIAL ACCESS.

DISTRIBUTED PROCESSING: Electronic data processing (EDP) performed in computers near or at the sources of data or near the users of results, in contrast to centralized data processing performed at a single, central site removed from data sources or users.

DNR (Dialed Number Recorder): A device used in a telephone switching office to record the numbers dialed from a preselected telephone.

DOWNLOAD: To transfer files from a remote computer system to the user's system.

DTR (Data Terminal Ready): A designation applied to a control circuit used in a terminal or computer to tell its modem that the terminal or computer is ready for operation.

EDP (Electronic Data Processing): Also called data processing (DP) and automated data processing (ADP) in the federal government.

EDP AUDITOR: A person who performs operational, computer, computer program, and data file reviews to determine the integrity, adequacy, performance, security, and compliance with organization and generally accepted policies, procedures, and standards. This person also may participate in design specification of applications to ensure adequacy of control.

EFTS (Electronic Funds Transfer System): A computer and telecommunication network used to execute monetary transfers.

E-MAIL (Electronic Mail): The use of computer and telecommunications systems for transmission of messages; a message sent from a computer terminal and addressed for delivery to one or more persons at their computer terminals.

ELECTRONIC DATA INTERCHANGE (EDI): The interchange of electronic forms of business documents such as purchase orders and invoices among business organization's computers.

ELECTRONIC LETTER BOMBS: A message sent from one computer terminal to another through a computer containing commands that cause the message to be sent back to the computer for execution as though it were a set of instructions from the keyboard of the receiving terminal.

EXPERT SYSTEM: A real-time computer application that uses artificial intelligence for a particular subject of inquiry.

FACILITIES ENGINEER: A person who inspects, adjusts, repairs, modifies, or replaces equipment supporting computer and terminal facilities (e.g., air conditioning, light, heat, power, water).

FIELD: Reserved space or storage for a set of characters.

FILE: A collection of related data records treated as a unit.

See: DATA SET.

FILE SERVER: A device used in a local area network (LAN) to provide storage of data files for other devices on the LAN.

FIRMWARE (computer jargon, not recommended for use): A computer program that is considered to be a part of a computer and not modifiable by computer operating system or application programs. It often makes use of computer instructions not available for normal programming. The name is derived from other jargon terms (software and hardware).

FORTRAN (FORmula TRANslation): A higher level programming language primarily used to write computer programs that tend to be more engineering-or scientific-oriented rather than business-oriented.

FREEWARE (computer jargon, not recommended for use): Computer program for which there is no charge.

FRONT-END PROCESSOR: A special-purpose computer attached to a main computer used to reduce the work load of the main computer primarily for input, output, and data communications functions.

4GL (Fourth Generation Language): Any computer programming language that is closest to the English language for coding specified applications.

HACKER: A person who views and uses computers as objects for exploration and exploitation.

HARD DISK: Computer storage disk made of rigid material and not meant for removal from a disk drive device.

HARDWARE (computer jargon, not recommended for use): The computer and all related or attached machinery, such as mechanical, magnetic, electrical, and electronic devices, used in data processing.

Contrast with: SOFTWARE.

HASH TOTAL: The sum in an abbreviated form of any set of data used to help assure the data are not changed.

See: CHECK SUM.

HIGH-LEVEL LANGUAGE: A programming language that is independent of the structure of any given computer or that of any given class of computers that is more similar to the language used by the programmer than to assembly or machine language. Some languages are designed for specialized applications.

Contrast with: ASSEMBLY LANGUAGE and MACHINE LANGUAGE.

INFORMATION: The meaning that a human assigns to data by means of conventions used in their representation; sometimes interchangeable in meaning with data.

See: DATA

INSTRUCTION: A statement appearing in a computer program that specifies an operation and the values or locations of its operands.

INSTRUCTION LOCATION: The place or address where data in the form of an instruction may be stored within a computer system.

INTERACTIVE: The mode of use of a computer system in which each action external to the computer system elicits a timely response. An interactive system may also be conversational, implying a continuous dialog between the user and the computer system.

I/O: Input to a computer and/or output from a computer.

I/O BOUND: The state of execution of a computer program in which the computer time for execution is determined by I/O activity rather than computation activity.

Contrast with: COMPUTATION BOUND.

IS (Information Systems): A general term to denote all the operations and procedures involved in a data processing system.

JCL: See JOB CONTROL LANGUAGE.

JOB: A set of data and computer programs that constitute a complete unit of work for a computer. A job usually includes all necessary computer programs, information for linking computer programs, data, files, and instructions to the operating system.

JOB CONTROL LANGUAGE: A programming language used to create job control statements. A job control program is a computer program that is used by the computer system to prepare each job or job step to be run.

JOB QUEUE: A sequenced set of jobs in computer storage arranged in order of assigned priority for execution by a computer.

JOB SETUP CLERK: A person who requests that jobs be executed, requests media libraries for necessary data, physically places jobs and data into job queues, handles procedures for reruns, and possibly distributes output to users.

LAN (Local Area Network): A network designed to provide facilities for inter-user communication within a small geographic location such as in one or several neighboring buildings. It may be connected to public facilities or other networks.

LAPTOP COMPUTER: A microcomputer that folds into or is contained in an easily carried small case about the size of an attache case.

LINE TRACE: Identification of a telephone that was or is being used to call a prespecified telephone number.

LOAD AND GO: A computer operations method by which higher level language programs or jobs are entered, prepared for execution. and immediately executed.

LOCAL PROCESSING: Data processing that is conducted near or at the user's location rather than at a remote CPU.

LOGIC BOMB: Computer instructions residing in a computer (usually within a Trojan horse program) that, when executed, determines conditions or states of a computer system that facilitates or triggers the perpetration of an unintended act.

LOOP: A sequence of instructions in a computer program that is executed repeatedly until a terminal condition prevails; also a local telephone circuit.

MANAGEMENT INFORMATION SYSTEM: See MIS.

MACHINE LANGUAGE: A computer language that is executed directly by a computer, without first having to pass through a translation program, such as a compiler.

MAGNETIC STORAGE: A computer data storage device using electromagnetic technology.

MAINFRAME COMPUTER: A medium-sized to large computer, usually requiring an environment with special temperature, humidity, and power controls.

MAIN STORAGE: The fastest access storage device in a computer system where the storage locations can be addressed by a computer program, and instructions and data can be moved from and into registers in the CPU from which the instructions can be executed or from which the data can be operated on.

MASTER FILE: A file of data that is used as an authority in a given job and that is relatively permanent, even though its contents may change from run to run.

MEDIA LIBRARIAN: A person who files, retrieves, and accounts for off-line storage of data on disk, tape, cards, or other removable data storage media. The person provides media for the production control and job set-up areas and functions, and cycles backup files through remote storage facilities.

MEDIUM: The material, or configuration thereof, on which data are recorded. Examples are punched paper tape, punch cards, magnetic tape, and disks.

MEMO UPDATE: A file update procedure whereby master files are not directly modified to reflect each transaction. Instead, pointers to other files are used to keep track of updates to specified records. Pointers are used periodically to obtain the data to merge with and update a master file.

MEMORY: See MAIN STORAGE.

MICR (Magnetic Ink Character Recognition): A standard machine-readable type font printed with magnetic ink on documents such as bank checks and deposit slips that can be directly read by machine.

MICROCOMPUTER: A small computer consisting of a microprocessor, storage, keyboard, display screen, and other I/O devices; generally known as a personal or desktop computer.

MINICOMPUTER: Larger than a microcomputer and smaller than a mainframe computer.

MIS (Management Information System): An integrated man/machine computer system for providing information to support the operations, management, and decision-making functions in an organization; also used as the name of a department that provides computer services.

MLS (Multi-Level Security): Confidential, secret, and top secret classifications in the U.S. government.

MODEM (MOdulator-DEModulator): A device that modulates and demodulates signals transmitted over data telecommunication facilities and that converts between analog and digital representations of data. It functions between a digital computer and an analog communication circuit.

MONITOR: Unit in large computers that prepares the machine instructions from the source program, using built-in compiler(s) for one or more program languages, and feeds these into the processing and output units in sequence, once compilation is completed; also controls time-sharing procedures.

MULTIPROCESSING: The use of two or more CPUs in a computer system under integrated control.

MULTIPROGRAMMING: The execution of two or more programs accomplished by sharing the resources of a computer.

NETWORK: See COMPUTER NETWORK.

OBJECT CODE: Output from a compiler or assembler that is executable machine language.

Contrast with: SOURCE CODE.

OCR (Optical Character Recognition): The machine identification of printed characters through use of light-sensitive devices.

Contrast with: MICR.

ON-LINE: The state of devices or computer users in direct communication with a CPU; also a computer system in an interactive or time-sharing mode with people or other processes.

OPERATING SYSTEM: An integrated collection of computer programs resident in a computer that supervise and administer the use of computer resources to execute jobs automatically.

OPERATIONS MANAGER: The manager of a computer facility responsible for the operation of the computer system, perhaps also responsible for the maintenance, specification, acquisition, modification, security, and replacement of computer systems or computer programs.

OPTICAL DATA STORAGE: A computer data storage device using laser optics technology.

PACKET-SWITCHED COMMUNICATION: A data communication protocol in which packets of addressed data are sent and retrieved based on the embedded address.

PARALLEL PROCESSING: Concurrent processing of one program on several CPUs.

PC (Personal Computer): A microcomputer with enough memory, I/O devices, and processing capability to be used for small but complete applications and word processing.

PEN REGISTER: A device used in a telephone switching office to record the telephone numbers of calls received by a preselected telephone.

See: DNR.

PERIPHERAL EQUIPMENT OPERATOR: A person who operates devices attached to or in conjunction with the computer that performs data I/O functions.

PHONE PHREAK (also FREAK): A person who uses switched, dialed-access telephone services as objects for exploration and exploitation.

PIGGYBACKING (also TAILGATING): A method of gaining unauthorized physical access to guarded areas when control is accomplished by electronically or mechanically locked doors; also a method of tapping and using a data communications line when it is in standby mode.

PIN (Personal Identification Number): A password that must be entered by a computer system terminal user to gain access to a specific application program or service; most often associated with retail computer banking devices such as automated teller machines (ATMs).

PL/1: A high-level computer programming language designed for use in a wide range of business and scientific computer applications.

POS (POINT-OF-SALE) TERMINAL: Computer terminal used for transaction recording, credit authorization, and funds transfer; typically situated with merchant establishments at the point of retail sales.

PRODUCTION PROGRAM: A debugged and tested program that is beyond the development stage; often part of a library of programs used for data processing.

PROGRAM: See COMPUTER PROGRAM.

PROGRAMMER: A person who designs, writes, debugs, tests, and documents computer programs.

PROM (Programmable Read Only Memory): A memory that can be programmed by electrical pulses, after which it is read only.

RAM (Random Access Memory): A memory from and into which the user can read or write; "main" memory.

See: ROM.

REAL-TIME: The actual time during which a physical process transpires.

RECORD: A set of data fields.

REMOTE JOB ENTRY (RJE): Submission of jobs through an input unit that has access to a computer through a data communications link.

REMOTE PROCESSING: Data entry and partial or complete processing near the point of origin of a transaction. Remote processing systems typically edit and prepare data input before transmission to a central computer.

ROM (Read-Only Memory): A storage device in which the data content is fixed, readout is nondestructive, and data are retained indefinitely even when the power is shut off. In contrast, RAMs are capable of read and write operations, have nondestructive readout, but stored data are lost when the power is shut off.

RPG (Report Program Generator): A high-level computer programming language that is report rather than procedure-oriented. Programmers describe the functions desired of the computer by describing the output report.

RS232: Standard cable connector.

RUN BOOK: A document or computer data file containing instructions for computer operators detailing operations setup procedures, job schedule checklists, action commands, error correction and recovery instructions, I/O dispositions, and system backup procedures.

SALAMI TECHNIQUE: The unauthorized, covert process of taking small amounts (slices) of money or otherwise numeric value from many sources in and with the aid of a computer.

SCANNING: The process of presenting sequentially changing information to an automated system to identify those items that receive a positive response. The items are commonly telephone numbers or passwords that are used for computer intrusion.

SCAVENGING: A covert, unauthorized method of obtaining information that may be left in or around a computer system after the execution of a job. Included here is physical search (of trash barrels for carbon copies, for example) and search for residual data within the computer storage areas, temporary storage tapes, and the like.

SECURITY OFFICER: A person who evaluates, plans, implements, operates and maintains physical, operational, procedural, personnel, and technical safeguards and controls.

SEQUENTIAL ACCESS: An access method for storing or retrieving data according to their sequential order in a storage device.

Contrast with: DIRECT ACCESS.

SHOULDER SURFING: A spying technique of observing the screen or keyboard from behind a terminal operator to gain information.

SIMULATION AND MODELING IN A CRIME: The use of a computer as a tool for planning or controlling a crime (e.g., simulation of an existing computer process to determine the possibility of success of a premeditated crime).

SOFTWARE (computer jargon, not recommended for use): A set of computer programs, procedures, and sometimes including associated documentation.

Contrast with: COMPUTER PROGRAM, OPERATING SYSTEM.

SOURCE CODE: Instructions written by a programmer or computer user in a computer programming language that are used as input for a compiler, interpreter, or assembler.

Contrast with: OBJECT CODE.

SPOOLING: The reading and writing of data for I/O on auxiliary storage devices, concurrently with execution of other jobs, in a format for later processing or output operations.

SPREAD SHEET: A report produced by a nonsequential program where each entry in the report is discretely programmed by formulas.

STORAGE: A device used for retaining data or computer programs in machine-readable and retrievable form.

See: RAM, ROM, and MAIN STORAGE.

STORAGE CAPACITY: The number of bits, characters, bytes, words, or other units of data that a particular storage device can contain.

SUPERZAPPING: The unauthorized use of utility computer programs that violate computer access controls to cause loss of confidentiality, integrity, or availability of data in a computer or its services. The name derives from an IBM utility program called "Superzap."

SYSTEM ENGINEER: A person who designs, configures, tests, diagnoses, assembles and disassembles, and repairs or replaces computer system devices and components.

SYSTEMS PROGRAMMER: A person who designs, develops, installs, modifies, documents, and maintains operating system and utility programs.

TAILGATING: See PIGGYBACKING.

TELECOMMUNICATION: Any communication of information in verbal, written, coded, or pictorial form by telephony.

TELEPROCESSING: The processing of data that are received from or sent to remote locations by way of telecommunication circuits.

TELEPROCESSING MONITOR: A computer operating system program that controls the transfer of data between the communication circuits and a computer and often does the user polling (turn-taking among users) as well.

TERMINAL ENGINEER: A person who tests, diagnoses, assembles and disassembles, repairs, and replaces terminals or their components.

TIME-SHARING: A method of using a computing system that allows a number of users to execute programs as though concurrently and to interact with the programs during execution.

See: BATCH PROCESSING.

TRANSACTION OPERATOR: A person who operates a computer transaction terminal by entering transactions for processing by a computer system.

TRANSACTION SYSTEM: A computer system that is used for processing transactions in a prescribed manner controlled by application programs.

TRAP DOOR: A function, capability, or error in a computer program or equipment that facilitates compromise or unintended acts in a computer system.

TROJAN HORSE: Computer instructions secretly inserted in a computer program so that when it is executed in a computer, unintended acts are performed.

UNIX™: An operating system designed by Bell Laboratories for use with minicomputers and small business computers, and widely adopted by many manufacturers.

UPC (Universal Product Code): See BAR CODE.

UPDATE-IN-PLACE: A method for the modification of a master file with current data each time a transaction is received in a computer system.

Contrast with: MEMO UPDATE.

UPLOAD: Transferring data from a microcomputer or terminal to a mainframe.

UTILITY PROGRAM: A computer program designed to perform a commonly used function, such as moving data from one storage device to another.

VDT: Video Display Terminal.

VIRUS: A set of computer instructions that propagates copies or versions of itself into computer programs or data when it is executed.

VOLUME: A set of data files.

WIRETAPPING: Interception of communications signals with the intent to gain access to information transmitted over communications circuits.

WHEELWARS: A game played by two or more hackers with the objective of excluding all other players from system access.

WIZARD: A highly competent computer technologist or programmer.

WORD: A sequence of adjacent characters or bits considered as an entity in a computer.

WORKSTATION: A computer terminal and any collection of attached devices used by an information worker.

ZAP, ZAPPING: See SUPERZAPPING.

SECTION I: Classifying the Crime

This manual for investigation of computer crime and for prosecution of the perpetrator addresses technological forms of well-known crimes. Experience and legislative interest have shown that basing the treatment of computer crime on computer technology is often of value for the criminal justice and computer-using communities. Many computer crimes can be prosecuted successfully without delving deeply into the technology. Many more of them, however, involve sufficiently different occupations of perpetrators, environments, modi operandi, forms of assets lost, time scales, and geography from traditional crimes to identify the subject as a unique type of crime that warrants explicit capabilities and action.

This introductory section covers the following subjects:

- The changing nature of computer crime
- Working definitions of computer abuse, computer-related crime, and computer crime
- Classifications of computer crime
- A brief history of computer crime and an overview of investigation and prosecution experience.
- Relationships of white collar crime and computer crime.

A. The Nature of Computer Crime

Business, economic, and white-collar crimes have rapidly changed as computers proliferated into the activities and environments in which these crimes occur. Computers have engendered a different form of crime.

The evolution of occupations in this field has extended the traditional categories of criminals to include computer programmers, computer operators, tape librarians, and electronic engineers who function in new environments. Although crime has traditionally occurred in ordinary human environments, some crime is now perpetrated inside personal computers in bedrooms or mainframe computers in the specialized environment of rooms with raised flooring, lowered ceilings, large grey boxes, flashing lights, moving tapes, and the hum of air-conditioning motors.

The methods of committing crime have changed. A new jargon has developed, identifying automated criminal methods such as data diddling, Trojan horses, logic bombs, salami techniques, superzapping, piggybacking, scavenging, data leakage, and asynchronous attacks (see Section II). The forms of many of the targets of computer crime are also different. Electronic transactions and money, as well as paper and plastic money (credit cards), represent assets subject to intentionally caused, automated loss. Money in the form of electronic signals and magnetic patterns is stored and processed in computers and transmitted over telephone lines. Money is debited and credited to accounts inside computers. In fact, the computer has become the vault for the business community. Many other physical assets, including inventories of products in warehouses and of materials leaving or entering factories, are represented by electronic and optical documents of record inside computer systems. Electronic data interchange (EDI), which connects trading partners for conducting contract negotiations, sales, invoicing, and collections, focus traditional sources of business crime on computers and data communications.

The timing of some crimes is also different. Traditionally, the time of criminal acts is measured in minutes, hours, days, weeks, months, and years. Today, some crimes are being perpetrated in less than 0.003 of a second (3 milliseconds). Thus, automated crime must be considered in terms of a computer time scale of milliseconds (thousandths), microseconds (millionths), and nanoseconds (billionths) because of the speed of the execution of instructions in computers.

Geographic constraints do not inhibit perpetration of this crime. A telephone with an attached computer terminal in one part of the world could be used to engage in a crime in an on-line computer system in any other part of the world.

All these factors and more must be considered in dealing with the crime of computer abuse. Unfortunately, however, the business community, constituting all businesses, government agencies, and institutions that use computers for technical and business purposes, is neither adequately prepared to deal with nor sufficiently motivated to report this kind of crime to the authorities. Although reliable statistics are as yet unavailable to prove this, computer security studies for the business community and interviews with certified public accountants have indicated that few crimes of this type are ever reported to law enforcement agencies for prosecution. Many business people complain that even when they do report this crime, prosecutors frequently refuse to accept the cases for a variety of reasons, including their lack of understanding of the technology and their already heavy case loads. Prosecutors and investigators counter that the victim's records and documentation of crimes associated with computers in the

business community are inadequate for effective prosecution. In addition, many investigators are not sufficiently technically skilled and, even if they become so, are soon transferred to other, unrelated crime investigations.

B. Definition of Computer Crime

Computers have been involved in most types of crime, including fraud, theft, larceny, embezzlement, bribery, burglary, sabotage, espionage, conspiracy, extortion, attempted murder, manslaughter, pornography, trespassing, violation of privacy, and kidnapping. Criminal justice agencies having limited experience with computer crime generally think of it as crime that occurs inside computers. This narrow definition has recently broadened as computers proliferate into most societal functions. The public media have added to the confusion through sometimes sensationalized or inaccurate reporting.

Computer crime is not well understood in the criminal justice and computer-using communities, and no consensus on its definition exists, as evidenced by the diversity of state and federal computer crime laws. One definition is that it is a form of white-collar crime committed inside a computer system; another definition is that it is the use of a computer as the instrument of a business crime.

State and federal criminal codes contain at least 50 statutes defining computer crime (see Section VI). Any violations of these specific statutes are computer crimes under the most strict interpretation of the term; in some contexts it is also customary to include alleged violations of these statutes as computer crimes.

Computer-related crimes—a broader category—are any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution. Although computer-related crimes are primarily white-collar offenses, any kind of illegal act based on an understanding of computer technology can be a computer-related crime. They could even be violent crimes that destroy computers or their contents and thereby jeopardize human life (for example, of people who depend on the correct functioning of computers for their health or well being). The proliferation and use of personal computers make computer-related crimes potentially endemic throughout society.

Computer abuse encompasses a broad range of intentional acts that may or may not be specifically prohibited by criminal statutes. Any intentional act involving knowledge of computer use or technology is computer abuse if one or more perpetrators made or could have made gain and/or one or more victims suffered or could have suffered loss.

For purposes of this manual, the simplest term computer crime has been used to refer generally to all three categories: computer crime in the strict sense, computer-related crime, and computer abuse. Where the context requires distinctions among the three categories to avoid confusion or misinterpretation, the text specifically identifies the type of crime or abuse that is intended.

Computer crime may involve computers not only actively but also passively when usable evidence of the acts resides in computer stored form. The victims and potential victims of computer crime include all organizations and people who use or are affected by computer and data communication systems, including people about whom data are stored and processed in computers.

All known and reported cases of computer crime involve one or more of the following four roles:

- Object—Cases include destruction of computers or of data or programs contained in them or supportive facilities and resources such as air-conditioning equipment and electrical power that allow them to function.
- Subject—A computer can be the site or environment of a crime or the source of or reason for unique forms and kinds of assets lost such as a pirated computer program. A fraud perpetrated by changing account balances in financial data stored in a computer makes the computer the subject of a crime.
- Instrument—Some types and methods of crime are complex enough to require the use of a computer as a tool or instrument. A computer can be used actively such as in automatically scanning telephone codes to make unauthorized use of a telephone system. It could also be used passively to simulate a general ledger in the planning and control of a continuing financial embezzlement.
- Symbol—A computer can be used as a symbol for intimidation or deception. This could involve an organization falsely claiming to use nonexistent computers.

The dimensions of the definition of computer crime become a problem in some cases. If a computer is stolen in a simple theft where based on all circumstances it could have been a washing machine or milling machine and made no difference, then a knowledge of computer technology is not necessary, and it would not be a computer crime. However, if knowledge of computer technology is necessary to determine the value of the article taken, the nature of possible damage done in the taking, or the intended use by the thief, then the theft would be a computer crime.

To illustrate, if an individual telephones a bank funds transfer department and fraudulently requests a transfer of $70 million to his account in a bank in Vienna, two

possibilities occur. If the clerk who received the call was deceived and keyed the transfer into a computer terminal, the funds transfer would not be a computer crime. No fraudulent act was related directly to a computer, and no special knowledge of computer technology would be required. However, if the clerk was in collusion with the caller, the fraudulent act would include the entry of data at the terminal and would be a computer crime. Knowledge of computer technology would be necessary to understand the terminal usage and protocol.

These examples indicate the possibilities of rational conclusions in defining computer crime. However, more practical considerations should not make such explicit and absolute decisions necessary. If any information in this manual is useful for dealing with any kind of crime, its use should be encouraged.

C. Classification of Computer Crime

A classification of computer crime is based on a variety of lists and models from several sources to produce standards for categorization. The classification goes beyond white-collar crimes because, as stated above, computers have been found to be involved in almost all types of crime.

Efforts made in the mid-1970s to amend Title 18 of the U.S. Criminal Code resulted in Article 1030, Chapter 47, making crimes of unauthorized acts in, around, and with computers. Four main categories of computer crime were identified:

- The introduction of fraudulent records or data into a computer system.
- Unauthorized use of computer-related facilities.
- The alteration or destruction of information or files.
- The stealing, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data[2].

Computer crime has also been categorized by types of information and information-processing loss: modification, destruction, disclosure, and use or denial of use. This classification is deceptive, however, because many other types of loss have occurred, including acts of misrepresentation, delay or prolongation of use, renaming, misappropriation, and failure to act. Therefore, a more comprehensive and usable typing is loss of integrity, confidentiality, and availability of information. These three classes define acts that are intrinsic to information such as changing it, extrinsic to information such as changing access to it, and external to information by removing or copying it.

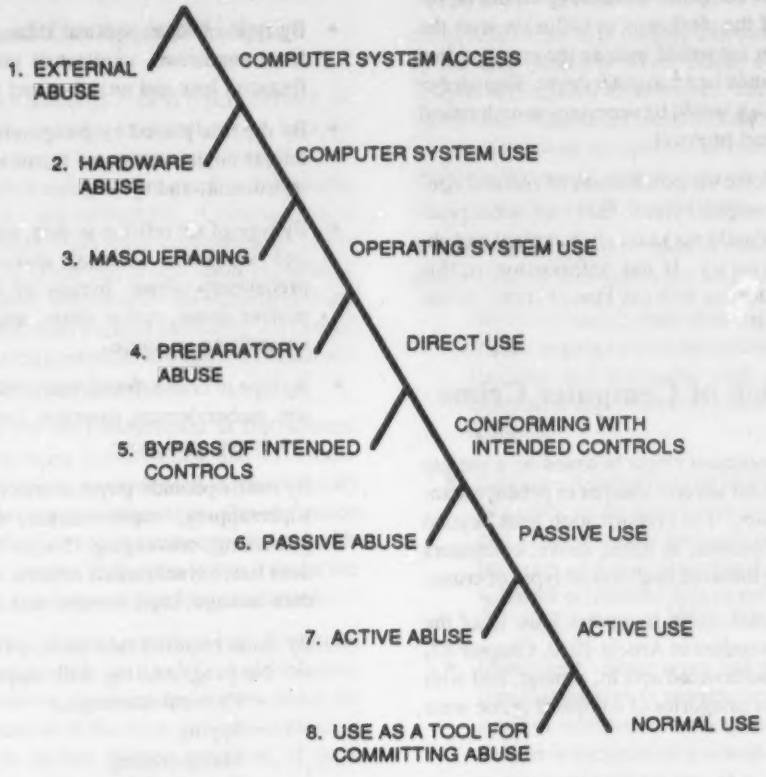
Computer abuse studies have identified categories in several dimensions:

- By ways in which information loss occurs: loss of integrity, confidentiality and availability.
- By type of loss: physical damage and destruction from vandalism, intellectual property loss, direct financial loss and unauthorized use of services.
- By the role played by computers: object of attack, unique environment and forms of assets produced, instrument, and symbol.
- By type of act relative to data, computer programs, and services: external abuse, masquerading, preparatory abuse, bypass of intended controls, passive abuse, active abuse, and use as a tool for committing an abuse.
- By type of crime: fraud, theft, robbery, larceny, arson, embezzlement, extortion, conspiracy, sabotage, espionage, and more.
- By modi operandi: physical attacks, false data entry, superzapping, impersonation, wire tapping, piggybacking, scavenging, Trojan horse attacks, trap door use, asynchronous attacks, salami techniques, data leakage, logic bombs, and simulation.
- By skills required (see Section II):
  - No programming skills required
    - Physical scavenging
    - Spying
    - Masquerading
    - Entering false data
    - Theft
  - Programming skills required
    - System scavenging
    - Eavesdropping
    - Scanning
    - Piggybacking and tailgating
    - Superzapping
    - Trojan horse attacks
    - Virus attacks
    - Salami attacks
    - Using trapdoors
    - Using logic bombs
    - Asynchronous attacks
    - Leaking data
    - Pirating
    - Use in criminal enterprises[1,3].

These classifications have been developed into sets of complete, detailed descriptions and models of computer crime. They are useful for a variety of research and practical purposes in investigation and prosecution of computer crime.

Figure 1

CLASSES OF COMPUTER ABUSE



The SRI Computer Abuse Methods Model considers a classification system for computer abuses that is summarized in Figure 1. It shows the relationships of the computer crime methods described in Section II. The model is more of a system of descriptors than it is a taxonomy in the usual sense, in that multiple descriptors may apply in any particular case. For visual simplicity this model is depicted as a simple tree, although that is an oversimplification—the classes are not mutually disjoint.

The order of categorization depicted is roughly from the physical world to the hardware to the operating system (and network software) to the application code. The first abuse class includes external abuses that can take place passively without access to the computer systems. The second class includes hardware abuse, and generally requires some sort of physical access and active behavior with respect to the computer system itself. Eavesdropping and interference are examples of these two classes, respectively. The third class includes masquerading in a variety of forms. The fourth includes cases of preparation for subsequent abuses, for example, the planting of a Trojan horse as opposed to the abuses that result from the actual exploitation of the Trojan horse—which show up later in subsequent classes. The remaining classes involve bypass of authorization, active abuse, passive abuse, and uses that lead to subsequent abuse. The leftward branches all involve misuses, while the rightward branches represent potentially acceptable use—until a leftward branch is taken. Every leftward branch represents a class of vulnerabilities that must be defended against, and detected at the earliest possible time. However, the techniques for defense and detection differ from one branch to the next.

This figure represents a classification system for types of techniques, but not a taxonomy of computer crimes. Actual violations of computer security and integrity have often involved multiple types of abuse. For example, the German Chaos Computer Club people who attacked NASA systems in 1987 utilized (at least) techniques of external abuse, masquerading, preplanned Trojan horse attacks, bypass of intended controls, and both active and passive abuses. Thus, the tree representation is merely a convenient way of summarizing the classes.

D. History of Computer Crime

Computer abuse started with the emergence of computer technology in the late 1940s. As the number of people in the computer field began to increase, that facet of human nature that wants to harm society for personal gain took hold; the problem of abuse became especially acute as computer technology proliferated into sensitive areas in society, such as military systems. The abuse then spread to engineering, to science, and in parallel business and personal applications.

The first recorded computer abuse occurred in 1958[1]. The first federally prosecuted computer crime, identified as such, was the alteration of bank records by computer in Minneapolis in 1966.

No valid, representative statistics on computer crime exist, even though several surveys have been conducted and well-known organizations and individuals have quoted various statistics. Frequency, losses per year, rate of increase or decrease, percentages of perpetrators within or outside victimized organizations, and the number of cases discovered and prosecuted are not known. To protect themselves, victims try to deny their loss. No methods have been devised to apply uniform definitions, identify authoritative sources, or conduct surveys in any statistically valid way. For example, the American Bar Association Task Force on Computer Crime, Section of Criminal Justice, reported the results of an informal questionnaire survey in a report on computer crime [40], but stated:

> One cannot extrapolate from the results of this limited survey to derive a valid "total annual dollar loss" figure for computer crime, a figure which has been sought by many, but which is elusive and unattainable given the current state of record-keeping...
>
> It is also noteworthy that many of the largest organizations responding to the survey (those with annual revenues/budgets over $1 billion) reported no available system to monitor or estimate value of losses...
>
> As various commentators have pointed out, valid and reliable statistics on the actual incidence of computer crime and actual losses sustained on any comprehensive basis are simply not possible until better reporting systems are in place.

Other statistical reports are "The Discovery and Prosecution of Computer Abuse: Assessing Information Systems Managerial Responses" by Detmar W. Straub, Jr., University of Minnesota Graduate School of Business (June 1987) and "Computer Crime, The First Annual Statistical Report," prepared by the National Center for Computer Crime Data, with Jay Bloombecker, editor (1986). As experience increases, valid statistics on rates of convictions among cases reported to the authorities should be obtainable, but only with respect to specific statutes.

Pursuit of the study of computer crime and computer abuse has been controversial. In 1970, a number of researchers concluded that the problem was merely a small part of the effect of technology on society and not worthy of specific, explicit research. The increase in substantial losses associated with intentional acts involving computers proved the fallacy of this view. The explicit identification of computer crime as a subject for research and development of preventative measures in criminal justice suffered a similar fate in the mid-1970s. Researchers argued that computers should not be the focus in a study of various types of crime. They believed the involvement of computers should be subordinate to the study of each specific type of crime, both manual and automated. The uniqueness of characteristics of computer crime across all the different types of crime was not considered sufficient to warrant explicit research.

The formal study of computer abuse was started in 1971. The first national conference on computer abuse and a comprehensive report were completed in 1973[1]. Since then, many reports, papers, journal articles, and books have been published describing the research[4, 5, 6].

The interest of the criminal justice community began in response to increasing numbers of cases and action by criminal justice organizations, including the FBI Academy, Criminal Justice Conferences on white-collar and organized crime, National District Attorneys Association Economic Crime Project, Postal Inspection, Secret Service, Securities and Exchange Commission, Internal Revenue Service, state and local criminal justice agencies, and the National College of District Attorneys. In 1976, the FBI established for its agents a 4-week training course in investigation of computer crime and another for other agencies in 1978. The U.S. Treasury, Federal Law Enforcement Training Center at Glynco, Georgia, is now the largest training facility for police officers that addresses computer crime.

In 1976, as a result of the increasing frequency of cases, Senator Abraham Ribicoff and his U.S. Senate Government Affairs Committee became aware of computer crime and the inadequacy of federal criminal law to deal with it. The committee produced two reports on its research[7, 8], and Senator Ribicoff introduced the first Federal Systems Protection Act Bill in June 1977. These legislative efforts evolved into House Bill 5616 in 1986, which resulted in the Computer Fraud and Abuse Act of 1987 established as Article 1030, Chapter 47 of Title 18 Criminal Code (see Appendix A). On the state level, Florida, Michigan, Colorado, Rhode Island, and Arizona were the first to have

computer crime laws based on the first Ribicoff bill. Current legislation on computer crime exists in 48 states (see Appendix B). The Florida, Colorado, Texas, New York, and California statutes are also included in Appendix A.

Computer crime has been portrayed fictionally in several novels, motion pictures, and television dramas. Two comic strips, Dick Tracy and Steve Roper, have depicted fictional stories. The British Broadcasting System dramatized the computer crime aspects of a massive insurance fraud. NBC TV News and the CBS show "60 Minutes" have had special segments. The motion picture "War Games" was the first to popularize computer hacking. Several nonfiction trade books have been published, and articles have appeared in all major magazines and newspapers. Unfortunately, the public interest and sensationalism associated with computer crime, particularly the malicious hacker cases that peaked in 1982 and the 1988 computer virus cases, has made folk heroes of the perpetrators and embarrassed the victims. Prosecutors have sometimes benefited from the visibility of their cases and the high conviction rate.

E. News Media Reporting of Computer Vulnerabilities

The news media have done a great service in bringing public attention to the problem of computer crime; however, investigators and prosecutors who must deal with the real and not only the reported nature of the problem should not be influenced by the media's sometimes distorted representations. Since 1970, a number of computer crime issues have saturated and subsequently faded from news media attention, while the potential for loss grows more serious as technology advances. The largest issues have been the following:

- Invasion of personal privacy
- Salami fraud techniques
- Telephone toll fraud
- Hacking computer intrusion
- Electronic letter bomb Trojan horse attacks
- Software piracy
- Interference with communications
- Radio frequency emanation monitoring
- Computer virus attacks.

News reporters often ask investigators and prosecutors for information on these cases, especially as the issues become popular and associated with celebrated people. Criminal justice personnel must be cautious to protect the privacy of victims, suspects, and witnesses, as well as the confidentiality of their cases and findings. Fortunately, journalists, through their increasing experience with computer use and computer technology, are becoming more accurate in their reporting of computer crimes. Appendix C describes selected cases of computer crime that have been reported in the news media.

F. Investigation and Prosecution Experience

Extensive fieldwork preceded the writing of the original edition (1979) of this manual. In particular, several weeks were spent interviewing 44 prosecutors and investigators in the Los Angeles District Attorney's office and several prosecutors in offices in New York City and Philadelphia. Their experiences in prosecuting computer crime and more than 50 cases were documented. A questionnaire survey of 49 prosecutors was also conducted[9]. The information obtained at that time has been used as the basis for parts of this manual. This revision of the manual, which is based on experience and studies occurring since 1979, incorporates results of a 1985 telephone survey of 100 prosecutors who have prosecuted computer crime; that survey was funded by the U.S. Department of Justice, Bureau of Justice Statistics[10]. It also incorporates the findings of a study of 200 reported computer abuses and the identification of 38 computer abuse techniques funded by an agency of the U.S. Department of Defense.

The initial reaction to inquiries about the deputy district attorneys' (DDAs) experiences with computer crime was that "we have had no computer crime cases." Further discussion usually indicated that they have had several crime cases in which computers had been involved to a significant extent, but DDAs had failed to classify them as computer crimes. This more recent study has indicated that although prosecutors are acknowledging more computer crimes, few of the perpetrators are being charged or prosecuted under the state computer crime statutes and for good reasons:

- The statutes are relatively new, untested, and unfamiliar to the courts and prosecutors.
- The penalties are generally weak compared to other statutes.
- Most computer crimes are successfully chargeable under other statutes when careful and adequate police investigation is performed (e.g., incriminating evidence on paper, positive identity of suspects).

The DDAs generally agreed that the number of computer crimes will increase. Moreover, because the defendants

and their defense attorneys understand the technical aspects, the prosecutors must also understand them. Technically knowledgeable investigators can materially help the prosecutor in this respect.

G. White Collar Crime and Computer Crime

1. Defining White Collar Crime

In its narrowest definition, white collar crime is composed of those crimes committed by individuals in the upper and middle social classes and/or certain high status occupations. Generally, these crimes involve acts that are nonviolent, principally involving elements of deceit, deception, concealment, corruption, misrepresentation, and/or breach of trust.

A more current general definition comes from Albert J. Reiss, Jr., and Albert D. Biderman[11]. They define white collar crime as a violation of law "that involves the use of a violator's position of significant power, influence or trust . . . for the purpose of illegal gain, or to commit an illegal act for personal or organizational gain."

A slightly different definition of white collar crime was adopted by the Congressional Subcommittee on Crime, Committee on the Judiciary. That definition is "an illegal act or series of illegal acts committed by nonphysical means and by concealment or guile, to obtain money or property, to avoid the payment of loss of money or property, or to obtain personal or business advantage." Congress adopted this definition in 1979 in the Justice System Administration Improvement Act.

2. Comparing White Collar Crime and Computer Crime

White collar crimes cover many acts that may, but need not, include the use of a computer as an essential element of the crime. Examples are antitrust violations, public corruption, bribes, environmental pollution, and price fixing. Computer crimes can also include white collar crimes but need not be limited to those types of acts. Examples of nonwhite collar crimes are virus attacks on computer systems, as well as acts of violence or unauthorized changes in computers that control industrial processes.

Computer crimes have a number of characteristics in common with other white collar crimes. Although the computer assists in the commission of the crime, the crime itself is not necessarily distinctive to computers or so unique that it will be unknown to law enforcement officials. Computer and white collar crimes have the following characteristics in common:

- Common law and criminal justice-related issues:
  - The crimes include a number of traditional civil or criminal violations, as well as certain new acts related to changing commercial/technological conditions, that legislators have defined as illegal after problems come to their attention.
  - These illegal acts are often regulatory or other types of specialized violations that do not fall under local police responsibilities.
  - Evidence is difficult to collect and easy to destroy, either purposely by a perpetrator or accidentally by investigators.
  - These crimes are often difficult to detect, with discovery quite often started by accident or customer complaint rather than as the result of direct investigation.
  - The media view these crimes as newsworthy, often creating great pressure on public officials to act quickly by making arrests and passing laws.
- Common criminal behavior-related issues:
  - Both types of acts are often committed through nonviolent means, although certain industrial, consumer, and environment-related crimes have life-threatening consequences.
  - Access to computers or computer storage media, through employment-related knowledge or technical skills, is often needed.
  - These acts often involve "respectable" persons who have not previously been convicted of any crime.
  - These acts generally involve information manipulations that either directly or indirectly create profits or losses.
  - These crimes can be committed by an individual, several individuals working in collusion, and/or organizations, with the victims in the latter case ranging from individual clients, customers, or employees of other organizations.
- Common organizational issues:
  - The general public views many of these acts as less serious than crimes involving physical violence. Exceptions to this view are the more serious types of white collar and computer crimes, including fraud against consumers, cheating on income taxes, environmental pollution by factories, price fixing, and public officials accepting bribes.

- These crimes cost individuals, organizations, and society large amounts of resources. Accurate estimates are impossible to determine because of the unknown number of crimes committed and the difficulty of defining associated losses.
- Prevention of these crimes requires a combination of legal, technical, managerial, security, and audit-monitoring controls.

3. Computer Crime Characteristics Unique from Other White Collar Crimes

Computer crimes differ from white collar crimes in certain other respects. These differences relate to the unique aspects of computer or related information processing development, as follows:

- Unique law and criminal justice-related issues:
  - Traditional laws are not always applicable to computer-related violations, making it difficult for prosecutors to decide how to proceed.
  - Determining the most appropriate statute to process these crimes can also be difficult.
  - Most law enforcement officials do not have sufficient knowledge to respond to this type of crime.
  - This type of crime is not a high-priority issue for most legislators or prosecutors, partly because of the lack of an active public or law enforcement constituency lobbying for improvements in response to computer crime.
- Unique criminal behavior-related issues:
  - In the past, only those with technical knowledge could commit computer crimes. Now, however, as computer access and user-friendly equipment become more widely available, the number of competent users has expanded.
  - Direct, face-to-face interaction is not necessary to commit this crime, and, with the development of direct international communications between computers, attempts at unauthorized access can occur across thousands of miles, numerous time zones, and national/jurisdictional boundaries.
  - The motivations behind these crimes include not only profit but also a wish to test the limits of technology, to politically attack corporations and societies, and to seek personal revenge against employers or individuals.
- Unique organizational issues:
  - These crimes can significantly embarrass the victimized business; frequently, the managers decide not to contact law enforcement officials and allow the perpetrators to quietly leave the corporation, with or without repayment of losses.
  - Detecting these crimes and collecting sufficient evidence are difficult tasks made even more complex because they necessitate active cooperation between businesses and law enforcement.

4. White Collar Crime Statistics

Recent figures on the prosecution of white collar offenders reveal important changes over the last several years[12, 13, 14]. These figures also suggest areas where basic statistics on computer crime prevention need to be collected.

Of those arrested by state or local police for white collar felonies in eight states and one territory in 1983,* 88% were prosecuted—about the same proportion as those arrested for felonies involving property crimes (86%), violent crimes (82%), and public-order/vice/disorderly conduct (81%).

Persons prosecuted for the white collar crimes of forgery/counterfeiting, fraud, and embezzlement had a conviction rate also about the same (74%) as those arrested for property crimes (76%), but higher than for violent crimes (66%), or public-order crimes (67%).

Criminal cases were filed by U.S. attorneys against 55% of white collar suspects, which is the same filing rate as for non-white collar offenses. The filing rate for tax fraud was the highest (79%), followed by regulatory offenses (65%). About 40% of white collar offenders convicted in 1985 were sentenced to incarceration, compared to 54% for non-white collar offenders. Those convicted of white collar crimes received shorter average sentences of incarceration (29 months) than other federal offenders (50 months). Those convicted of non-white collar crimes were more than twice as likely as white collar offenders to receive a sentence of more than 5 years; white collar offenders were more likely to be sentenced to probation or fined.

Among white collar offenders, those convicted of counterfeiting were the most likely to be sentenced to incarceration (59%). They received the longest average sentence (40 months) and were the most likely to be sentenced to more than 5 years.

When compared to previous years, these figures show that law enforcement agencies now treat white collar crime more seriously. Therefore, to the degree that white collar crime includes computer crime, increased serious treatment may apply to reported computer crime as well.

* Not necessarily representative of all jurisdictions.

SECTION II: Computer Abuse Methods and Detection

Investigators and prosecutors should deal with computer crime as much as possible in the context of their experience with other, more traditional crime. However, when computer technology plays a key role that sometimes cannot be avoided, a thorough understanding of abusive methods involving computers is essential. In addition, being aware of the types of people who have the skills and knowledge to use these methods, likely evidence of their use, and detection methods can be most helpful[15, 16].

This section describes 17 computer abuse methods in which computers play a key role. Although several of the methods are far more complex than the nonexpert will understand in detail, these brief descriptions should help investigators and prosecutors comprehend the information sufficiently well to interact with technologists who can provide the necessary expertise to deal with them. Most technologically sophisticated computer crimes will use one or more of these methods. However, no matter how complex the methods, the crimes will still fit into the categories familiar to the prosecutor. For an explanation of the technical terms used in this discussion, the reader is referred to Section VII, the glossary, or the index.

Like most aspects of computer technology, a jargon describing the now classical methods of computer abuse has developed. These are the technical methods for some of the more sophisticated and automated attacks. The results are loss of information integrity, confidentiality, and availability associated with the use of services, computer and communications equipment or facilities, computer programs, or data in computer systems. Depending on the meaning of the data, kinds of services, or purpose of the programs, the acts range over many known types of crime and abuse. The methods are not necessarily identifiable with specific statutory offenses. The methods, possible types of perpetrators, likely evidence of their use, and detection are described below.

A. Eavesdropping and Spying

Eavesdropping includes wiretapping and monitoring radio frequency emanations. Few wiretap abuses are known, and no cases of radio frequency emanation eavesdropping have been proven outside of government intelligence agencies. Case experience is probably so scarce because industrial spying and scavenging represent easier, more direct ways for criminals to obtain the required information. On the other hand, these passive eavesdropping methods may be so difficult to detect that they are frequently used but never reported. These abusive methods are described in the news media far more than they deserve; nevertheless, the opportunities to pick up emanations from isolated small computers and terminals, microwave circuits, and satellite signals continue to grow.

While eavesdropping, the perpetrators often do not know when the needed data will be sent; therefore, they must collect relatively large amounts of data and search for the specific items of interest. Identifying and isolating the communications circuit can also pose a problem for perpetrators. Intercepting microwave and satellite communications is even more difficult, primarily because complex, costly equipment is needed for interception and because the perpetrators must determine whether active detection facilities are built into the communication system.

Clandestine radio transmitters can be attached to computer components. They can be detected by panoramic spectrum analysis or second-harmonic radar sweeping. Interception of free-space radiation is not a crime unless disclosure of its fruits violates the Electronic Communications Privacy Act (ECPA) of 1986 or the Espionage Act. Producing radiation may be a violation of FCC regulations.

Intelligible emanations can be intercepted even from large machine rooms and at long distances using parametric amplifiers and digital filters. Faraday-cage shielding can be supplemented by carbon-filament adsorptive covering on the walls and ceilings. Interception of microwave spillage and satellite footprints is different since it deals with intended signal data emanation and could be illegal under the ECPA if the intercepts were proved to be communicated to a third party.

The ultimate solutions to eavesdropping are producing computer and communication equipment with reduced emanations and using cryptography to scramble data. Because both solutions are relatively costly, they will not be used until the risks are perceived to be sufficiently great or meeting a new level of standard of due care is achieved through changes in practices, regulation, or law.

Spying consists of criminal acquisition of information by covert observation. For example, shoulder surfing involves observing users at computer terminals as they enter or receive displays of sensitive information such as passwords. A gang of juvenile delinquents in Atlanta using binoculars obtained passwords in this fashion. Frame-by-frame analysis of video recordings to pick up personal identification numbers (PIN) being entered at automatic teller machines (ATMs) is also feasible.

One method to prevent both eavesdropping and spying is electronic shielding that uses a Faraday grounded electrical

conducting shield in the former method and physical shielding from view in the latter. Detection and obtaining evidence require that investigators observe the acts and capture equipment.

Eavesdropping should be assumed to be the least likely method used in the theft or modification of data. Detection methods and possible evidence will be the same as in the investigation of voice communication wiretapping. Table 1 summarizes the potential perpetrators, detection, and evidence in eavesdropping acts.

Table 1

DETECTION OF EAVESDROPPING

Potential Perpetrators	Methods of Detection	Evidence
Communications technicians and engineers	Voice wire tapping methods	Voice wire tapping evidence
	Observation	
Communications employees	Tracing sources of equipment used	

B. Scanning

Scanning is the process of presenting sequentially changing information to an automated system to identify those items that receive a positive response. This method is usually used to identify telephone numbers that access computers, user IDs, and passwords that facilitate access to computers, as well as credit card numbers that can be used illegally for ordering merchandise or services through telemarketing.

Scanning was vividly portrayed in the motion picture "War Games" where the hero used his microcomputer to automatically scan for telephone numbers that responded with computer data carrier tones. Computer programs that perform the automatic searching, called "Demon Programs," are available from various malicious hacker electronic bulletin boards. Scanning may be prosecuted as criminal harassment, but probably not trespass or fraud until the information identified is used with criminal intent. Scanning for credit card numbers involves testing sequential numbers by automatically dialing credit verification services. Access to proprietary credit rating services may constitute criminal trespass.

The perpetrators of scanning are mostly malicious hackers and potential computer system intruders. Many computer systems can deter scanners by limiting the number of access attempts. Trying to exceed these limits results in long delays meant to discourage the scanning process. Identifying the perpetrators is often difficult, usually requiring the use of pen registers or dialed number recorder (DNR) equipment in cooperation with communications companies. The possession of a Demon Program may constitute possession of a tool for criminal purposes, and printouts from Demon Programs may be used to incriminate a suspect.

C. Masquerading

Masquerading is the process of one person assuming the identity of an authorized computer user by acquiring identifying items, knowledge, or characteristics. Physical access to computers or computer terminals and electronic access through terminals to a computer require positive identification of an authorized user. The authentication of identity is based on some combination of something the user knows, such as a secret password; some physiological or learned characteristic of the user, such as a fingerprint, retinal pattern in the eye, hand geometry, keystroke rhythm, or voice; and a token the user possesses, such as a magnetic stripe card, smart card, or metal key. Anybody with the correct combination of identification characteristics can masquerade as another individual.

An example of a clever masquerade occurred when a young man posed as a magazine writer and called on a telephone company indicating that he was writing an article on the computer system in use by the telephone company. He was given a full and detailed briefing on all the computer facilities and application systems. As a result of this information, he was able to steal over $1 million worth of telephone equipment from the company.

In another case, an individual stole magnetic stripe credit cards that required secret PINs for each use. He would telephone the owners, stating that he was a bank official, had discovered the theft of the card, and needed to know the secret PIN to protect the victim and issue a new card. Victims invariably gave out their secret PINs, which the impersonator then used to withdraw the maximum amount allowed.

Playback is another masquerade and occasional piggyback method. User or computer responses or initiations of transactions could be surreptitiously recorded and played back to the computer as though they came from the user. Playback was suggested as a means of "jackpotting" ATMs by repeating cash dispensing commands to the machines through a wiretap. This fraud was curtailed when

banks installed controls that placed encrypted message sequence numbers, times, and dates into each transmitted transaction and command.

Computer masquerading as well as user masquerading can be used to obtain confidential information such as passwords from users or to give them false information. In one case a group of students notified all campus computer users in a mailed memo that the telephone number into the computer had been changed to a number of a telephone actually connected to a student's computer. After obtaining the users' passwords, the computer directed them back to the use of the correct number and promptly signed off.

Masquerading is the most common activity of computer system intruders. It is also one of the most difficult to prove in a trial. When an intrusion takes place in the victim's computer, the investigator must obtain evidence identifying the masquerader at a terminal as performing the acts producing the events in the computer. This task is doubly difficult when network weaving connections through several switched telephone systems interfere with pen register and DNR line tracing. Table 2 summarizes the methods of detecting computer abuse committed by masquerading.

Table 2

DETECTION OF MASQUERADING

Potential Perpetrators	Methods of Detection	Evidence
All computer users	Audit log analysis	Computer audit log
Hackers	Password violations	Notes and documents in possession of suspects
	Observation	Pen register and DNR records
	Report by person impersonated	Witnesses
		Access control package exception or violation reports

D. Piggybacking and Tailgating

Piggybacking and tailgating can be done physically or electronically. Physical piggybacking is a method for gaining access to controlled access areas when control is accomplished by electronically or mechanically locked doors. Typically, an individual carrying computer-related objects such as tape reels stands by the locked door. When an authorized individual arrives and opens the door, the piggybacker goes in after or along with him. Turnstyles, mantraps, or a stationed guard are the usual methods of preventing this type of unauthorized access. The turnstyle allows passage of only one individual with a metal key, an electronic or magnetic card key, or combination lock activation. A mantrap is a double-doored closet through which only one person can move with one key action. The success of this method of piggybacking depends on the quality of the access control mechanism and the alertness of authorized persons in resisting cooperation with the perpetrator.

Electronic piggybacking can take place in an on-line computer system where individuals are using terminals and the computer system automatically verifies identification. When a terminal has been activated, the computer authorizes access, usually on the basis of a secret password, token, or other exchange of required identification and authentication information (protocol). Compromise of the computer can occur when a covert computer terminal is connected to the same line through the telephone switching equipment and used when the legitimate user is not using his or her terminal. The computer will not be able to differentiate between the two terminals, but senses only one terminal and one authorized user. Piggybacking can also be accomplished when the user signs off or a session terminates improperly, leaving the terminal or communications circuit in an active state or leaving the computer in a state where it assumes the user is still active. Call fowarding of the victim's telephone to the perpetrator's telephone is another means of piggybacking.

Tailgating involves connecting a computer user to a computer in the same session as and under the same identifier as another computer user whose session has been interrupted. This situation happens when a dial-up or direct-connect session is abruptly terminated, and a communications controller (concentrator or packet assembler/disassembler) incorrectly allows a second user to be patched directly into the first user's still-open files. The problem is exacerbated if the controller incorrectly handles a modem's data-terminal-ready (DTR) signal. Many network managers set up the controller to send DTR signals continually so that the modem quickly establishes a new session after finishing its disconnect sequence from the previous session. The controller may miss the modem's drop-carrier signal after a session is dropped, allowing a new session to tailgate onto the old session.

In one vexing situation, some computer users connected their office terminal hard-wired cables directly to their personal modems, which allowed them to connect any outside

telephone directly to their employers' computers through central data switches, thus avoiding all dialup protection controls such as automatic callback devices. Therefore, people dialing their regular office numbers found themselves with a computer carrier signal answering and direct access to the computers. Such data switch pass-through methods are very dangerous and have few means of acceptable control.

Electronic door access control systems frequently are run by a microcomputer that produces a log showing accesses and time of accesses for each individual gaining access. Human guards frequently do equivalent journaling by keeping logs. Unauthorized access can be detected by studying journals and logs and by interviewing people who may have witnessed the unauthorized access. Table 3 summarizes the methods of detecting computer abuse committed by piggybacking and tailgating methods.

Table 3

DETECTION OF PIGGYBACKING AND TAILGATING

Potential Perpetrators	Methods of Detection	Evidence
Employees, former employees, vendor's employees	Access observations	Logs, journals, equipment usage meters
Contracted persons	Interviewing witnesses	Photos, voice, and video recordings
Outsiders	Examination of journals and logs	Other physical evidence
	Out-of-sequence messages	
	Specialized computer programs that analyze characteristics of on-line computer user accesses	

E. False Data Entry (Data Diddling)

False data entry is usually the simplest, safest, and most common method used in computer abuse. It involves changing data before or during their input to computers. Anybody associated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, and transforming data that ultimately enter a computer can change these data. Trusted, authorized computer users engaged in unauthorized activities are often the persons using the method. Examples of data diddling are forging, misrepresenting, or counterfeiting documents; exchanging valid computer tapes or disks with prepared replacements; keyboard entry falsifications; failure to enter data; and neutralizing or avoiding controls.

A typical example of false data entry is the case of a timekeeping clerk who filled out data forms of hours worked by 300 employees in a railroad company department. He noticed that all data on the forms entered into the timekeeping and payroll system on the computer included both the name and the employee number of each worker. However, the computer used only employee numbers for processing and even for printing employee names and addresses on payroll checks. He also noticed that outside the computer all manual processing and control was based only on employee names, because nobody identified people by their numbers. He took advantage of this dichotomy of controls by filling out forms for overtime hours worked, using the names of employees who frequently worked overtime but entering his own employee number. His false data entry was not discovered for years until by chance an auditor examining W-2 federal income forms noticed the clerk's unusually high annual income. An examination of the timekeeping computer files and data forms and a discussion with the clerk's supervisor revealed the source of the increased income. The clerk was confronted with the evidence and admitted his fraudulent activities. Well-designed timekeeping and payroll systems use the first few letters of employees' names appended to their identification numbers to reduce the likelihood of this type of crime.

Data are normally protected by manual methods; once data are in the computer, they can be automatically identified, validated, and verified. Manual controls include maker-checker-signer roles for trusted people with separation of responsibilities or dual responsibilities that force collusion to perpetrate fraudulent acts. Batch control totals can be manually calculated and compared in the computer with matching computer-produced batch control totals. In this method, data are batched into small groups, and data are added together to produce the control total. Another common control is the use of check digits or characters embedded in the data based on various characteristics of each field of data (e.g., odd or even number indicators or hash totals). Sequence numbers and time of arrival can be associated with data and checked to ensure that data have not been lost or reordered. Large volumes of data can be checked with utility or special-purpose programs. Evidence of data diddling is data that: (1) do not correctly represent data found at sources, (2) do not match redundant or duplicate data, and (3) do not conform to earlier forms of data if the manual

processes are reversed. Further evidence is control totals or check digits that do not check or meet validation and verification test requirements in the computer.

Potential data diddling perpetrators hold various kinds of occupations. Table 4 summarizes the likely perpetrators, the methods of detecting data diddling, and the sources of evidence.

Table 4

DETECTION OF FALSE DATA ENTRY

Potential Perpetrators	Methods of Detection	Evidence
Transaction participants Data preparers	Data comparison	Data documents Source Transactions Computer-readable
Source data suppliers	Document validation	
Nonparticipants with access	Manual controls	
	Audit log analysis	Computer data media Tapes Disks Storage modules
	Computer validation Reports analysis	
	Computer output comparison	
	Integrity tests (e.g., for value limits, logic consistencies, hash totals, crossfoot and column totals and forged entry)	Manual logs, audit logs, journals, and exception reports
		Incorrect computer output control violation alarms

F. Superzapping

Superzapping derives its name from Superzap, a macro or utility program used in most IBM mainframe computer centers as a systems tool. Any computer center that has a secure computer operating mode needs a "break-glass-in-case-of-emergency" computer program that will bypass all controls to modify or disclose any of the contents of the computer. Many Superzap types of programs for sale and in the public domain are also available and necessary for microcomputers as well. Computers sometimes stop, malfunction, or enter a state that cannot be overcome by normal recovery or restart procedures. Computers also perform unexpectedly and need attention that normal access methods do not allow. In such cases, a universal access program is needed. This situation parallels using a master key if all other keys are lost or locked in the enclosure they were meant to open.

Utility programs such as Superzap are powerful and dangerous tools in the wrong hands. They are normally used only by systems programmers and computer operators who maintain computer operating systems. They should be kept secure from unauthorized use; however, they are often placed in program libraries where they can be used by any programmer or operator who knows of their presence and how to use them.

A classic example of superzapping resulting in a $128,000 loss occurred in a New Jersey bank. The manager of computer operations was using a Superzap program to change account balances as directed by management for correcting errors. The regular error correction process was not working properly because the demand-deposit accounting system had become obsolete and error-ridden as a result of inattention in a computer changeover. After the operations manager discovered how easy it was to make changes without the usual controls or journal records, he transferred money to three friends' accounts. They engaged in the fraud long enough for a customer to find a shortage: quick action in response to the customer's complaint resulted in indictment and conviction of the perpetrators. The use of the Superzap program, which left no evidence of data file changes, made discovery of the fraud through technical means highly unlikely.

Unauthorized use of Superzap programs can result in changes to data files that are normally updated only by production programs. Usually, few if any controls can detect changes in the data files from previous runs. Application programmers do not anticipate this type of fraud; their universe of concern is limited to the application program and its interaction with data files. Therefore, the fraud will be detected only when the recipients of regular computer output reports from the production program notify management that a discrepancy seems to have occurred. Computer managers will often conclude that the evidence indicates data entry errors, because it would not be a characteristic computer or program error. Considerable time can be wasted in searching the wrong areas. When management concludes that unauthorized file changes have occurred independent of the application program associated with the file, a search of all computer usage journals might reveal the use of a Superzap program, but this is unlikely if the perpetrator anticipates the possibility. Occasionally, there may be a record of a request to have the file placed on-line in the computer system if it is not normally in that mode. Otherwise, the changes would have to occur when the production program using the file is being run or just before or after it is run.

Superzap acts may be detected by comparing the current file with father and grandfather copies of the file where no updates exist to account for suspicious changes. Table 5 summarizes the potential perpetrators, methods of detection, and sources of evidence in superzapping abuse.

Table 5

DETECTION OF SUPERZAPPING

Potential Perpetrators	Methods of Detection	Evidence
Programmers with access to Superzap programs and computer access to use them	Comparison of files with historical copies	Output report discrepancies
Computer operations staff with applications knowledge	Discrepancies noted by recipients of output reports	Undocumented transactions
	Examination of computer usage journals	Computer usage or usage or file request journals

G. Scavenging and Reuse

Scavenging is a method of obtaining or reusing information that may be left in or around a computer system after processing. Simple physical scavenging could be the searching of trash barrels for copies of discarded computer listings or carbon paper from multiple-part forms. More technical and sophisticated methods of scavenging include searching for residual data left in a computer or computer tapes and disks after job execution.

In the 1987 Iran-Contra affair, Lt. Col. Oliver North did not understand that using the ERASE command in the White House Executive E-mail system merely removed the name and storage address of an E-mail message from the directory of messages; it did not destroy the contents of the message. In addition, frequent backup copies of all messages were made and stored for later retrieval in the event of a computer failure. As a result, much of his correspondence was retrieved as evidence of possible wrongdoing.

Computer systems are designed and operators are trained to preserve data, not destroy them. If computer operators are requested to destroy the contents of disks or tapes, they will most likely make backup copies first. This situation offers opportunities for both criminals and investigators alike.

A computer operating system may not properly erase buffer storage areas or cache memories used for the temporary storage of input or output data. Many operating systems do not erase magnetic disk or magnetic tape storage media because of the excessive computer time required to do this. Therefore, new data are written over the old data. (The data on optical disks cannot electronically be erased, although additional bits could be burned in to a disk to change data or effectively erase them by making all 0s into 1s.)

The next job might be executed to read the data from previous jobs before they are replaced by new data. In a poorly designed operating system, if storage were reserved and used by a previous job and then assigned to the next job, the next job would gain access to the same storage, write only a small amount of data into that storage, but then read the entire storage area back out for its own purposes, thus capturing—scavenging—data that were stored by the previous job.

In one case, a time-sharing service in Texas had a number of oil companies as customers. The computer operator noticed that every time one particular customer used computer services his job always requested that a scratch tape (temporary storage tape) be mounted on a tape drive. When the operator mounted the tape, the read-tape light always came on before the write-tape light came on, indicating that the user was reading data from a temporary storage tape before he had written anything on it. After numerous such incidents, the computer operator reported the circumstances to management. Simple investigation revealed that the customer was engaged in industrial espionage, obtaining seismic data stored by various oil companies on the temporary tapes and selling these highly proprietary, valuable data to other oil companies.

Scavenging is often detected through the discovery of suspected crimes involving proprietary information that may have come from a computer system and computer media. The information may be traced back to its source and originating computer usage, although the act was more likely a manual scavenging of information in human-readable form or the theft of magnetic tapes or disks rather than electronic scavenging.

In another case, valuable data were found on continuous forms from a computer output printer. Each page of the output had a preprinted sequence number and the name of the paper company. An FBI agent traced the paper back to the paper company, and, on the basis of the type of forms and sequence numbers, from there to the computer center where the paper had been used. The sequence numbers led to a specific printer and time at which the forms were printed. Identifying the job that produced the reports at that time and the programmer who submitted the job from the computer console log and usage accounting data was straightforward.

Table 6 lists the potential perpetrators. The table also summarizes the methods of detecting and the kinds of evidence typical with scavenging techniques.

Table 6

DETECTION OF SCAVENGING CRIMES

Potential Perpetrators	Methods of Detection	Evidence
Users of the computer system	Tracing of discovered proprietary information back to its source	Computer output media (page numbers and vendor)
Persons having access to computer or backup facilities and adjacent areas	Testing of an operating system to discover residual data after job execution	Type font characteristics
		Similar information produced in suspected ways in the same form

H. Trojan Horses

The Trojan horse method is the covert placement or alteration of computer instructions or data in a program so that the computer will perform unauthorized functions but usually still allow the program to perform most or all of its intended purposes. The Trojan horse program, which can be the carrier of many abusive acts, is the primary method used for inserting instructions for other abusive acts such as logic bombs, salami attacks, and viruses. It is the most commonly used method in computer program-based frauds and sabotage. Instructions may be placed in production computer programs so that they will be executed in the protected or restricted domain of the program and have access to all of the data files that are assigned for the program's exclusive use. Programs are usually constructed loosely enough to allow space to be found or created for inserting the instructions, sometimes without even extending the length or changing the check sum of the infected program.

One Trojan horse technique, called the electronic letter bomb attack, received great attention in the news media in 1981 because its use would have made most computers with terminal-to-terminal communication vulnerable to compromise. Some computers and terminals were changed to be resistant to this type of attack. Even though many computers are still wide open to attack, no cases of the method being used for criminal purposes have been reported.

The attack method consists of sending messages to other terminals with embedded control characters ending with the send line or block mode command (depending on the type of terminals being used). When the messages reach the display memory of intelligent terminals, the send line or block mode command is sensed, and the entire message is sent back to the computer for execution of the embedded control character commands as though they came from the victim at the receiving terminal with all of his computer access authority.

Such attacks can be prevented in two ways. The send line or block mode type of commands can be removed from all terminals allowed access to the computer, or a logic filter can be placed in the computer operating system to prevent all control character commands from being sent in terminal-to-terminal messages. Neither solution is particularly desirable because important and useful capabilities are lost.

Assuring detection and prevention of Trojan horse methods is impossible if the perpetrator is sufficiently clever, although practical methods are available for reducing the likelihood of, preventing, and detecting Trojan horse attacks. A typical business application program can consist of more than 100,000 computer instructions and data. The Trojan horse can also be concealed among as many as 5 or 6 million instructions in the operating system and commonly used utility programs. There it waits for execution of the target application program, inserts extra instructions in it for a few milliseconds of execution time, and removes them with no remaining evidence. Even if the Trojan horse is discovered, there is almost no indication of who may have done it. The search can be narrowed to those programmers who have the necessary skills, knowledge, and access among employees, former employees, contract programmers, consultants, or employees of the computer or software suppliers.

A suspected Trojan horse might be discovered by comparing a copy of the operational program under suspicion with a master or other copy known to be free of unauthorized changes. Backup copies of production programs are routinely kept in safe storage, but clever perpetrators will make duplicate changes in them. In addition, programs are frequently changed for authorized purposes without the backup copies being updated, thereby making comparison difficult. A program suspected of being a Trojan horse can sometimes be converted from object form into assembly or higher level form for easier examination or comparison by experts. Utility programs are usually available to compare large programs, but their integrity and the computer

system on which they are executed must be assured by qualified and trusted experts.

A Trojan horse might also be detected by testing the suspect program with a wide range of data that might expose the purpose of the Trojan horse. However, the probability of success is low unless exact conditions for discovery are known. Moreover, the computer used for testing must be conditioned to prevent loss to other data or programs. This testing may prove the existence of the Trojan horse, but usually will not determine its location. A Trojan horse may also reside in the source language version or only in the object form and may be inserted in the object form each time it is assembled or compiled—for example, as the result of another Trojan horse in the assembler or compiler. Use of foreign computer programs obtained from untrusted sources such as freeware bulletin board systems should be restricted, and the programs should be carefully tested before production use.

The methods for detecting Trojan horse frauds are summarized in Table 7. The table also lists the occupations of potential perpetrators and the sources of evidence of Trojan horse abuse.

Table 7

DETECTION OF TROJAN HORSE CRIMES

Potential Perpetrators	Methods of Detection	Evidence
Programmers having detailed knowledge of a suspected part of a program and its purpose and access to it	Program code comparison	Unexpected results of program execution
Employee technologists	Testing of suspect program	Foreign code found in a suspect program
Contract programmers	Tracing of unexpected events or possible gain from the act to suspected programs and perpetrators	Audit Logs
Vendors' programmers	Examination of computer audit logs for suspicious programs or pertinent entries	Uncontaminated copies of suspect programs
Computer operators		

I. Computer Viruses

A computer virus is a set of computer instructions that propagates copies or versions of itself into computer programs or data when it is executed within unauthorized programs. The virus may be introduced through a program designed for that purpose (called a pest) or a Trojan horse: hidden instructions are inserted into a computer program, the data, or the computer hardware itself that the victim uses. The hidden virus propagates itself into other programs when they are executed, creating new Trojan horses, and may also execute harmful processes under the authority of each unsuspecting computer user whose programs or system have become infected. A worm attack is a variation in which an entire program replicates itself throughout a computer or computer network.

Prevention of computer viruses therefore depends on protection from Trojan horses or unauthorized programs, and recovery after introduction of a virus entails purging all modified or infected programs and hardware from the system. The timely detection of a Trojan horse virus attack depends on the alertness and skills of the victim, the visibility of the symptoms, the motivation of the perpetrator, and the sophistication of the perpetrator's techniques. A sufficiently skilled perpetrator with enough time and resources could anticipate most known methods of protection from Trojan horse attacks and subvert them.

Although the virus attack method has been recognized for at least 15 years, it was first reported in a 1983 technical paper prepared by Prof. Fred Cohen, a computer scientist at the University of Cincinnati. The first three cases were reported in November 1987. Of the hundreds of cases that occur, most are in academic, research, and malicious hacker cultures. However, disgruntled employees or ex-employees of computer program manufacturers have contaminated products during delivery to customers.

A rich mixture of terminology about computer viruses has developed from the field of biological viruses and communicable diseases. Antivirus computer programs such as "Vaccination," "FluShot," "Data Physician," "Antidote," and "Virus RX" are being sold with both narrow and broad spectrum effectiveness.

Prevention methods consist primarily of investigating the sources of untrusted software and testing of foreign software in computers that have been conditioned to minimize possible losses. Prevention and subsequent recovery after an attack are similar to those for any Trojan horse. The system containing the suspected Trojan horse should be shut down and not used until experts have determined the sophistication of the abuse and the extent of damage. The investigator needs to determine whether the more common hardware and software errors or the very rare intentionally produced Trojan horse attacks have occurred.

Investigators should first interview the victims to identify the nature of the suspected attack. They should also use the special tools available (not resident system utilities) to examine the contents and state of the system after a suspected event (see Appendix E). The original provider of the programs suspected of being contaminated should be consulted to determine whether others have had similar experiences. Without a negotiated liability agreement, however, the vendor may decide to withhold important, possibly damaging information. Other users of the products could also be contacted as independent sources of information with mutual interests.

Possible indications of a virus infection include the following:

- The file size may increase when a virus attaches itself to the program or data in the file.
- An unexpected change in the time of last update of a program or a file may indicate a recent unauthorized modification.
- Several executable programs that all have the same date and/or time in the last update field indicate they have all been updated together, possibly by a virus.
- A sudden, unexpected decrease in free disk space may indicate sabotage by a virus attack.
- Unexpected disk accesses, especially in the execution of programs that do not use overlays or large data files, may indicate virus activity.

All current conditions at the time of discovery should be documented (using documentation facilities separate from the system in use). Next, if possible, all physically connected and inserted devices and media that are locally used should be removed. If the electronic domain includes remote facilities under the control of others, an independent means of communication should be used to report the event to the remote facilities manager. Computer operations should be discontinued; accessing system functions could destroy evidence of the event and cause further damage. For example, accessing the contents or directory of a disk could trigger the modification or destruction of its contents. Data can be recovered without destruction, but special tools and skills are required.

To protect themselves against viruses or indicate their presence, users can perform the following activities:

- Compare programs or data files that contain check sums or hash totals with backup versions to determine possible integrity loss.
- Compare system interrupt vectors (internal control tables) to spotlight any unusual and unexpected activity.
- Write-protect diskettes whenever possible and especially when testing an untrusted computer program. Unexpected write-attempt errors may indicate serious problems.
- Scan computer program source listings to reveal unexpected character strings that may be used by viruses to taunt their victims.
- Test untrusted programs with the computer system clock set at some future date to determine if a time bomb is present.
- Boot diskette-based systems using clearly labeled boot diskettes.
- Avoid booting a hard disk-drive system from a diskette.
- Never put untrusted programs in hard disk root directories. (Most viruses can affect only the directory from which they are executed; therefore, untrusted computer programs should be stored in isolated directories containing a minimum number of other sensitive programs or data files.)
- In local area network environments, avoid placing untrusted computer programs in common file server directories.
- Limit access to the file server node to authorized network administrators.
- When transporting files from one computer to another, use diskettes that have no executable files that might be infected.
- When sharing computer programs, share source code rather than object code since source code can more easily be scanned for unusual contents.
- Be aware that many commercially available antivirus programs are limited in the range of viruses they detect. [Some antivirus programs interfere with the normal operation of programs they are supposed to protect (e.g., blocking a disk formatting utility). In addition, an antivirus program may warn of a suspected infection when none has taken place.]

The best protection against viruses, however, is to frequently back up all important data and programs, maintaining multiple backups over a period of time, possibly up to a year, to be able to recover from uninfected backups. Trojan horse programs or data may be buried deeply in a computer system such as in disk sectors that have been declared by the operating system as unusable. In addition, viruses may contain counters for logic bombs with high values, meaning that the virus may be spread many times before its earlier copies are triggered to cause visible damage.

The perpetrators, detection, and evidence are the same as for the Trojan horse attack.

J. Salami Techniques

An automated form of abuse using the Trojan horse method or secretly executing an unauthorized program that causes the unnoticed or immaterial debiting of small amounts of assets from a large number of sources or accounts is identified as a salami technique (taking small slices without noticeably reducing the whole). Other methods must be used to remove the acquired assets from the system. For example, in a banking system the demand deposit accounting system of programs for checking accounts could be changed (using the Trojan horse method) to randomly reduce each of a few hundred accounts by 10 cents or 15 cents by transferring the money to a favored account where it can be withdrawn through authorized, normal methods. No controls are violated because the money is not removed from the system of accounts. Instead, small fractions of the funds are merely rearranged. The success of the fraud is based on the idea that each checking account customer loses so little that it is of little consequence or goes unnoticed. Many variations are possible. The assets may be an inventory of products or services as well as money. Few reported cases are known.

One salami method in a financial system is known as the "round down" fraud. Although no proven cases have ever been reported, it is a frequent topic of discussion and provides insights into the general method. The round down fraud requires a computer system application where large numbers of financial accounts are processed. The processing must involve the multiplication of dollar amounts by numbers—such as in interest rate calculations. This arithmetic results in products that contain fractions of the smallest denomination of currency, such as the cent in the United States. For example, a checking account in a bank may have a balance of $15.86. Applying a 2.6% interest rate results in adding $0.41236 ($15.86 × .026) to the balance for a new balance of $16.27236. However, because the balance is to be retained only to the nearest cent, it is rounded down to $16.27, leaving $0.00236. What is to be done with this remainder? The interest calculation for the next account in the program sequence might be the following: $425.34 × 0.026 = $11.05884. This would result in a new balance of $436.39884 that must be rounded up to $436.40, leaving a deficit or negative remainder of $0.00116, usually placed in parentheses to show its negative value ($0.00116).

The net effect of rounding in both these accounts, rounding down to the calculated cent in the first and adding 1 cent in the second, leaves both accounts accurate to the nearest cent and a net remainder of $0.0012 ($0.00236-$0.00116). This remainder is then carried to the next account calculation, and so on. As the calculations continue, if the running or accumulating remainder goes above 1 cent, positive or negative, the last account is adjusted to return the remainder to an amount less than 1 cent. This scheme results in a few accounts receiving 1 cent more or less than the correct rounded values, but the totals for all accounts remain in balance.

In these circumstances creative computer programmers can engage in some trickery to accumulate for themselves a regular flow of relatively small amounts of money and still show a balanced set of accounts that defies discovery by the auditor. These programmers use the Trojan horse method to slightly change the instructions in the program by accumulating the rounded down remainders in their own account rather than distributing them to the other accounts as they build up.

Using a larger number of accounts shows how this fraud would be committed. First, if rounded down correctly, the accounts would be as shown in Table 8. The interest rate applied to the total of all accounts, $3,294.26, results in a new total balance of $3,379.91 ($3,294.26 × 1.026) and a remainder of $0.00076 when the new total balance is rounded. The program calculates this figure as verification that the arithmetic performed account by account is correct. However, note that several accounts (those marked with an asterisk) have 1 cent more or less than they should have.

Table 8

EXAMPLE OF ROUNDED DOWN ACCOUNTS

Old Balance	New Balance	Rounded New Balance	Remainder	Accumulating Remainder
$ 15.86	$ 16.27236	$ 16.27	$ 0.00236	$ 0.00236
425.34	436.39884	436.40	(0.00116)	0.00120
221.75	227.51550	227.52	(0.00450)	(0.00330)
18.68	19.16568	19.17	(0.00432)	(0.00762)
564.44*	579.11544	~~579.12~~	(0.00456)	(0.01218)
		579.11		(0.00218)
61.31	62.90406	62.90	0.00406	0.00188
101.32	103.95432	103.95	0.00432	0.00620
77.11*	79.11486	~~79.11~~	0.00486	0.01106
		79.12		0.00106
457.12	469.00512	469.01	(0.00488)	(0.00382)
111.35	114.24510	114.25	(0.00490)	(0.00872)
446.36*	457.96536	~~457.97~~	(0.00464)	(0.01336)
		457.96		(0.00336)
88.68	90.98568	90.99	(0.00432)	(0.00768)
14.44*	14.81544	~~14.82~~	(0.00456)	(0.01224)
		14.81		(0.00224)
83.27	85.43502	85.44	(0.00498)	(0.00722)
127.49	130.80474	130.80	0.00474	(0.00248)
331.32	339.93432	339.93	0.00432	0.00184
37.11	38.07486	38.07	0.00486	0.00670
111.31*	114.20406	~~114.20~~	0.00406	0.01076
		114.21		0.00076
$3294.26		$3379.91		

Now suppose a programmer writes the program to accumulate the round amounts into his own account, the last account in the list. The calculations will be as shown in Table 9. The totals are the same as before, and the verification shows no tinkering. However, now the new balances of some accounts are 1 cent less, but none are 1 cent more as in the previous example. Those extra cents have been accumulated and all added to the programmer's account rather than to the accounts where the adjusted remainder exceeded 1 cent.

Table 9

EXAMPLE OF ROUNDED DOWN ACCOUNTS CONVERTED TO PROGRAMMER'S ACCOUNT

Old Balance	New Balance	Rounded New Balance	Remainder	Accumulating Remainder	Programmer's Remainder
$ 15.86	$ 16.27236	$ 16.27	$ 0.00236	$ 0.00000	$0.00236
425.34	436.39884	436.40	(0.00116)	(0.00116)	0.00236
221.75	227.51550	227.52	(0.00450)	(0.00566)	0.00236
18.68	19.16568	19.17	(0.00998)	(0.00998)	0.00236
564.44*	579.11544	~~579.43~~	(0.00456)	(0.01454)	0.00236
		579.11		(0.00454)	
61.31	62.90406	62.90	0.00406	(0.00454)	0.00642
101.32	103.95432	103.95	0.00432	(0.00454)	0.01074
77.11	79.11486	79.11	0.00486	(0.00454)	0.01560
457.12	469.00512	469.01	(0.00488)	(0.00942)	0.01560
111.35*	114.24510	~~114.35~~	(0.00490)	(0.01432)	0.01560
		114.24		(0.00432)	
446.36	457.96536	457.97	(0.00464)	(0.00896)	0.01560
88.68*	90.98568	~~90.98~~	(0.00432)	(0.01328)	0.01560
		90.98		(0.00328)	
14.44	14.81544	14.82	(0.00456)	(0.00784)	0.01560
83.27*	85.43502	~~85.44~~	(0.00498)	(0.01282)	0.01560
		85.43		(0.00282)	
127.49	130.80474	130 80	0.00474	(0.00282)	0.02034
331.32	339.93432	339.93	0.00432	(0.00282)	0.02466
37.11	38.07486	38.07	0.00486	(0.00282)	0.02952
111.31*	114.20406	~~114.30~~	0.00406	(0.00282)	0.03358
		114.23		0.00076	0.00000
		$3294.26		$3379.91	

Clearly, if there were 180,000 accounts instead of the 18 accounts in this example, the programmer could have made a profit of $300 ($0.03 × 10,000). Over several years, the fraud could cause significant loss.

Auditors might discover this fraud in only two known ways. They could check the instructions in the program, or they could recalculate the interest for the programmer's account after the computer executed the program. A clever programmer could easily disguise the instructions causing the fraudulent calculations in the program in a number of ways. However, this disguise would probably be unnecessary because no one would likely wade step by step through a program as long as use of the program showed no irregularities.

This program method would show no irregularities unless the programmer's account were audited, an unlikely event given that his account was one among 180,000. Besides, the programmer could have opened the account using a fictitious name or the name of an accomplice. He could also occasionally change to other accounts to further reduce the possibility of detection. Account activity unsupported by paper documents such as deposit slips could be audited but at great cost.

Experienced accountants and auditors indicate that the round down fraud technique has been known for many years, even before the use of computers. They say that a good auditor will look for this type of fraud by checking for deviations from the standard accounting method for rounding calculations.

Salami acts are usually not fully discoverable within obtainable expenditures for investigation. Victims have usually lost so little individually that they are unwilling to expend much effort to solve the case. Specialized detection routines can be built into the suspect program, or snapshot storage dump listings could be obtained at crucial times in suspected program production runs. If the salami acts are taking identifiable amounts, these can be traced, but a clever perpetrator will randomly vary the amounts or accounts debited and credited. Using an iterative binary search of balancing halves of all accounts is another costly way to isolate an offending account.

The actions and lifestyles of the few people and their associates who have the skills, knowledge, and access to perform salami acts can be closely watched for aberrations or deviations from normal. This technique could be successful because observable actions are usually required to convert the results to obtainable gain. The perpetrators or their accomplices will usually withdraw the money from the accounts in which it accumulates in legitimate ways. Records will show an imbalance between the deposit and withdrawal transactions, but all accounts would have to be balanced relative to all transactions over a significant period of time to detect discrepancies. This is a monumental and expensive task.

Many financial institutions require employees to use only their financial services and make it attractive for them to do so. Employees' accounts are more completely and carefully audited than others. Such requirements usually force the salami perpetrators to open accounts under assumed names or arrange for accomplices to commit the fraud. Detection of suspected salami frauds might be more successful if investigators concentrate on the actions of possible suspects rather than on technical methods of discovery.

Table 10 lists the methods of detecting the use of salami techniques. The table also lists potential perpetrators and sources of evidence of the use of the technique.

Table 10

DETECTION OF SALAMI TECHNIQUES

Potential Perpetrators	Methods of Detection	Evidence
Financial system programmers	Detailed data analysis using a binary search	Many small financial losses
Employee technologists	Program comparison	Unsupported account balance buildups
Former employees	Transaction audits	Trojan horse code
Contract programmers	Observation of financial activities of possible suspects	Changed or unusual personal financial practices of possible suspects
Vendor's programmers		

K. Trap Doors

When developing large application and computer operating systems, programmers insert debugging aids that provide breaks in the code for insertion of additional code and intermediate output capabilities much as scaffolding and temporary braces are used in building construction. Computer operating systems are designed so as to prevent unintended access to them and insertion or modification of code. Consequently, programmers will sometimes insert code that allows them to compromise these requirements during the debugging phases of program development and later during system maintenance and improvement. Programmers often have unexecuted, redundant, or incomplete instructions and unused data or parameters in their program code. These facilities are referred to as trap doors that can be used for Trojan horse and direct attacks such as false data entry. Normally, trap doors are eliminated in the final editing, but sometimes they are overlooked or intentionally left in to facilitate future access and modification. In addition, some unscrupulous programmers introduce trap doors for later compromising of computer programs. Designers or maintainers of large complex programs may also introduce trap doors inadvertently through weaknesses in design logic.

The most celebrated recent case of a serious flaw was found in the password-checking algorithm in the original UNIX™ Version 6, namely, the ability to construct universal passwords that would provide access for any legitimate user ID on any UNIX™ system. Somewhat simplified, the flaw was the failure to invoke bounds checking on the password input field. This failure facilitated the entry of a double length password, the first half consisting of any character string and the second half consisting of the encrypted form of the chosen password. Lack of a bounds check allowed the UNIX™-stored encrypted form of the authorized password stored previously in the field adjacent to the password to be overwritten by the encrypted form of the false password. The algorithm then encrypts the false password and compares it with the false password in encrypted form that was overwritten into the field adjacent to the password field. The comparison will always be successful[17].

Trap doors may also be introduced in the electronic circuitry of computers. For example, not all of the combinations of codes may be assigned to instructions found in the computer and documented in the programming manuals. When these unspecified commands are used, the circuitry may cause the execution of unanticipated combinations of functions that allow the computer system to be compromised.

Typical and known trap door flaws in computer programs include the following:

- Incomplete, inconsistent parameter validation and control of parameter and variable variance, limit, and range checks
- Implicit sharing of privileged data
- Asynchronous change between time of check and time of use
- Inadequate serialization
- Inadequate identification, verification, authentication, and authorization of tasks
- Failure to prevent exceeding programmed limits of capabilities and capacities
- Logic errors (e.g., more conditions or outcomes than branches)
- Incomplete design and specification
- Undocumented control transfers
- Control bypass or misplacement
- Improper naming, aliases
- Contextual dependencies
- Incomplete encapsulation
- Alterable audit trails
- Mid-process control transfers
- Hidden and undocumented application calls and parameters, operating system commands, and hardware instructions

- Failure to eliminate data residues or otherwise protect them
- Hidden or undocumented side effects
- Improper deallocation
- Ignored external device disconnect
- Incomplete aborts
- Embedded operating system parameters in application memory space
- Failure to remove debugging aids before production use begins.

During the use and maintenance of computer programs and computer circuitry, ingenious programmers invariably discover some of these weaknesses and take advantage of them for useful and innocuous purposes. However, the trap doors may also be used for unauthorized, malicious purposes as well. Functions that can be performed by computer programs and computers that are not in the specifications are often referred to as negative specifications. Designers and implementers struggle to make programs and computers function according to specifications and to prove that they do. They cannot practicably prove that a computer system conforms to negative specifications and does not perform functions that it is not supposed to perform. Conditions are too numerous to test.

Research is continuing on a high-priority basis to develop methods of proving the correctness of computer programs and computers according to complete and consistent specifications. However, it will likely be many years before commercially available computers and computer programs can be proved correct. Trap doors continue to exist; therefore, computer systems are fundamentally insecure because their actions are not totally predictable.

In one computer crime, a systems programmer discovered a trap door in a FORTRAN (FORmula TRANslation) programming language compiler. The trap door allowed the programmer writing in the FORTRAN language to transfer control from his FORTRAN program into a region of storage used for data. The computer instructions formed by the data could be secretly executed each time the FORTRAN program was run. The systems programmer in this commercial time-sharing computer service, in collusion with a user of the service, could use large amounts of computer time free of charge and obtain data and programs of other time-sharing users.

In another case, several automotive engineers in Detroit discovered a trap door in a commercial time-sharing service in Florida that allowed them to search uninhibitedly for privileged passwords. After discovering the password of the president of the time-sharing company, they obtained copies of trade-secret computer programs that they proceeded to use free of charge.

In both of these cases the perpetrators were discovered accidentally. It was never determined how many other users were taking advantage of the trap doors.

No direct technical method can be used to discover trap doors. However, when the nature of a suspected trap door is sufficiently determined, tests of varying degrees of complexity can be performed to discover hidden functions used for malicious purposes. This testing requires the expertise of systems programmers and knowledgeable application programmers. People without sufficient expertise attempting to discover trap door usage could waste large amounts of computer services and time. Investigators should always seek out the most highly qualified experts for the particular computer system or computer application under suspicion.

The investigator should always assume that the computer system and computer programs are never sufficiently secure from intentional, technical compromise. However, these intentional acts usually require the expertise of only the very few technologists who have the skills, knowledge and access to perpetrate them. Table 11 lists the potential perpetrators, methods of detection, and sources of evidence of the use of the trap door technique.

Table 11

DETECTION OF TRAP DOOR CRIMES

Potential Perpetrators	Methods of Detection	Evidence
Systems programmers	Exhaustive testing	Computer performance or output reports indicating that a computer system performs outside of its specifications
Expert application programmers	Comparison of specification to performance	
	Specific testing based on evidence	

L. Logic Bombs

A logic bomb is a set of instructions in a computer program executed at appropriate or periodic times in a computer system that determines conditions or states of the computer that facilitate the perpetration of an unauthorized, malicious act. In one case, for example, secret computer instructions were inserted (a Trojan horse) in the computer operating system where they were executed periodically. The instructions would test the year, date, and time of day clock in the computer so that on a specified day and time of the year the time bomb, a type of logic bomb, would trigger the

printout of a confession of a crime on all 300 computer terminals on-line at that time and then cause the system to crash. This act was timed so that the perpetrator would be geographically distant from the computer and its users. In another case, a payroll system programmer put a logic bomb in the personnel system so that if his name were ever removed from the personnel file, indicating termination of employment, secret code would cause the entire personnel file to be erased.

A logic bomb can be programmed to trigger an act based on any specified condition or data that may occur or be introduced. Logic bombs are usually placed in the computer system using the Trojan horse method. Ways to discover logic bombs in a computer system would be the same as for Trojan horses. Table 12 summarizes the potential perpetrators, methods of detection, and kinds of evidence of logic bombs.

Table 12

DETECTION OF LOGIC BOMBS

Potential Perpetrators	Methods of Detection	Evidence
Programmers having detailed knowledge of a suspected part of a program and its purpose and access to it Employees Contract programmers Vendors' programmers Computer users	Program code comparisons Testing of suspect program Tracing of possible gain from the act	Unexpected results of program execution Foreign code found in a suspect program

M. Asynchronous Attacks

Asynchronous attack techniques take advantage of the asynchronous functioning of a computer operating system. Most computer operating systems function asynchronously based on the services that must be performed for the various computer programs executed in the computer system. For example, several jobs may simultaneously call for output reports to be produced. The operating system stores these requests and, as resources become available, performs them in the order in which resources are available to fit the request or according to an overriding priority scheme. Therefore, rather than executing requests in the order they are received, the system performs them asynchronously based on resources available.

Highly sophisticated methods can confuse the operating system to allow it to violate the isolation of one job from another. For example, in a large application program that runs for a long time, checkpoint restarts are customary. These automatically allow the computer operator to set a switch manually to stop the program at a specified intermediate point from which it may later be restarted in an orderly manner without losing data. To avoid the loss, the operating system must save the copy of the computer programs and data in their current state at the checkpoint. The operating system must also save a number of system parameters that describe the mode and security level of the program at the time of the stop. Programmers or computer operators might be able to gain access to the checkpoint restart copy of the program, data, and system parameters. They could change the system parameters such that on restart the program would function at a higher priority security level or privileged level in the computer and thereby give the program unauthorized access to data, other programs, or the operating system. Checkpoint restart actions are usually well documented in the computer operation or audit log, however.

Even more complex methods of attack could be used besides the one described in this simple example, but the technology is too complex to present here. The investigator should be aware of the possibilities of asynchronous attacks and seek adequate technical assistance if suspicious circumstances result from the activities of highly sophisticated and trained technologists. Evidence of such attacks would be discernible only from unexplainable deviations from application and system specifications, in computer output, or characteristics of system performance. Table 13 lists the potential perpetrators and methods of detecting asynchronous attacks.

Table 13

DETECTION OF ASYNCHRONOUS ATTACKS

Potential Perpetrators	Methods of Detection	Evidence
Sophisticated advanced system programmers	System testing of suspected attack methods	Output that deviates from normally expected output or logs containing records of computer operation
Sophisticated and advanced computer operators	Repeat execution of a job under normal and safe circumstances	

N. Data Leakage

A wide range of computer crime involves the removal of data or copies of data from a computer system or computer facility[18]. This part of a crime may offer the most dangerous exposure to perpetrators. Their technical act may be well hidden in the computer; however, to convert it to economic gain, they must get the data from the computer system. Output is subject to examination by computer operators and other data processing personnel who might detect the perpetrators' activity.

Several techniques can be used to secretly leak data from a computer system. The perpetrator may be able to hide the sensitive data in otherwise innocuous looking output reports, by adding to blocks of data, for example. In more sophisticated ways the data could be interspersed with otherwise routine data. An even more sophisticated method might be to encode data to look like something different than they are. For example, a computer listing may be formatted so that the secret data are in the form of different lengths of printer lines, number of words or numbers per line, locations of punctuation, embedded in the least significant digits of engineering data, and use of code words that can be interspersed and converted into meaningful data. Another method is to control and observe the movement of equipment parts, such as the reading and writing of a magnetic tape causing the tape reels to move clockwise and counterclockwise in a pattern representing binary digits 0 and 1. A person watching the movement of the tape reels obtains the data. Similar kinds of output might be accomplished by causing a printer to print and skip lines in a pattern where the noise of the printer, recorded with a cassette tape recorder, might be played back at slow speed to produce a pattern translatable into binary information.

These rather exotic methods of data leakage might be necessary only in high-security, high-risk environments. Otherwise, much simpler manual methods might be used. It has been reported that hidden in the central processors of many computers used in the Vietnam War were miniature radio transmitters capable of broadcasting the contents of the computers to a remote receiver. These were discovered when the computers were returned to the United States from Vietnam.

Data leakage would probably best be investigated by interrogating data processing personnel who might have observed the movement of sensitive data. In addition, computer operating system usage journals could be examined to determine if and when data files may have been accessed. Because data leakage can occur through the use of Trojan horse, logic bomb, and scavenging methods, the use of these methods should be investigated when data leakage is suspected. Evidence will most likely be in the same form as evidence of the scavenging activities described above. Table 14 summarizes the detection of crimes resulting from data leakage.

Table 14

DETECTION OF CRIMES FROM DATA LEAKAGE

Potential Perpetrators	Methods of Detection	Evidence
Computer programmers	Discovery of stolen information	Computer storage media
Employees	Tracing computer storage media back to the computer facility	Computer output forms
Former employees		Type font characteristics
Contract workers		Trojan horse or scavenging evidence
Vendor's employees		

O. Computer Program Piracy

Piracy is defined here to mean the copying and use of computer programs in violation of copyright and trade secret laws. Commercially purchased computer programs are protected by what is known as a shrink-wrap contract agreement such as the following:

> This software product is copyrighted and all rights are reserved by X Corporation. The distribution and sale of this product are intended for the use of the original purchaser only and for use only on the computer system specified. Lawful users of this product are hereby licensed only to read the programs on the system and system backup disks from their medium into the memory of a computer solely for the purpose of executing them. Copying, duplicating, selling, or otherwise distributing this product is a violation of the law, except that the tutorial disk may be copied and distributed without further permission from or payment to X Corporation.

Since the early 1980s, violations of these agreements have been widespread, primarily because of the high price of commercial programs and the simplicity of copying the programs. The software industry reacted by developing several technical methods of preventing the copying of

disks, but these failed because of the hacker's skill at overcoming this protection and the customer's inconvenience.

The software industry has now stabilized and converged on a strategy of imposing no technical constraints to copying, implementing an extensive awareness program to convince honest customers not to engage in piracy, pricing their products more reasonably, and providing additional benefits to purchasers of their products that would not be obtainable to computer program pirates. In addition, computer program manufacturers occasionally find gross violations of their contract agreements and seek highly publicized remedies.

Malicious hackers commonly engage in piracy, sometimes even distributing pirated copies on a massive scale through electronic bulletin boards. Although criminal charges can often be levied against malicious hackers and computer intruders, industry most often seeks indictments against educational and business institutions, where gross violations of federal copyright laws and state trade secret laws are endemic.

Table 15

DETECTION OF COMPUTER PROGRAM PIRACY

Potential Perpetrators	Methods of Detection	Evidence
Any purchasers and users of commercially available computer programs	Observation of computer users	Pictures of computer screens while pirated software is being executed
Hackers	Search of computer users' facilities and computers	Copies of computer media on which pirated programs are found
	Testimony of legitimate computer program purchasers	Memory contents of computers containing pirated software
	Receivers of copied computer programs who testify to whom they have given additional copies	Printouts produced by execution of pirated computer programs

Investigators can most easily obtain evidence of piracy by confiscating suspects' disks, the contents of their computer hard disks, paper printouts from the execution of the pirated programs, and pictures of screens produced by the pirated programs. Note that recent court decisions indicate that piracy can also occur when programs are written that closely duplicate the "look and feel" of protected computer programs. The look and feel includes the use of similar command structures and screen displays. Table 15 summarizes the potential perpetrators, detection methods, and evidence of computer program piracy.

P. Computer and Computer Components Larceny

The theft, burglary, and sale of stolen microcomputers and components are increasing dramatically, a severe problem because the value of the contents of stolen computers often exceeds the value of the hardware taken. The increase in computer larceny is becoming epidemic, in fact, as the market for used computers in which stolen merchandise may be fenced also expands.

In one case a burglar discovered irreplaceable business records stored in a 20-megabyte hard disk in the computer that he stole. Feeling some remorse, he copied the content of the disk onto 20 diskettes and returned them by mail to the victim.

In another case a well-organized gang burglarized the storefront field offices of a large insurance company. In a 5-month period they stole 145 IBM AT computers valued at $800,000 (not counting consequential losses and potential loss of customer privacy). The gang could break into an office and remove an unprotected AT computer in less than 3 minutes. Many of the computers were protected by antitheft devices sealed to the tops of desks. After first stealing the AT by cutting out the entire section of the desktop, the gang found a way to force the computers out of the protective casings without damaging the computer case. In addition, the burglars interchanged the paper stickers on the back of the cases that show the AT's serial numbers. (In other instances, fencers have printed their own counterfeit serial number tags.) The burglary gang was caught through undercover police purchases of stolen computers and tracing the fencing trail to the gang leaders, who were subsequently convicted.

An additional method of protection other than normal office equipment antitheft security has been suggested. If the user is to be out of the office, microcomputers can be made to run antitheft programs that send frequent signals through modems and telephones to a monitoring station that would activate an alarm if the signals stopped.

Investigation and prosecution of computer larceny fits well within accepted criminal justice practices, except for proving the size of the loss when a microcomputer worth only a few hundred dollars is stolen. Evidence of far larger losses (e.g., programs, data) may be needed.

Minicomputers and mainframe computers have also been reported stolen. Typically, these cases occur while equipment is being shipped to customers. Existing criminal justice methods can deal with such thefts.

Q. Use of Computers for Criminal Enterprise

A computer can be used as a tool or instrument in a crime for planning, data communications, or control. Like any other business, complex white-collar and organized crimes often require the use of a computer. An existing process can be simulated on a computer, a planned method for carrying out a crime can be modeled, or a crime can be regulated by a computer to help assure its success.

In one case involving a million dollar embezzlement, an accountant owned his own service bureau and simulated his employer company's accounting and general ledger system on his computer. He could input both correct data and modified data to determine the effects of the embezzlement on the general ledger. He also could run the simulation in the reverse direction by inputting to the computer the general ledger data he wished to have. He then ran the system in reverse to determine the false entries in accounts payable and accounts receivable that would result in the required general ledger output.

In one phase of an insurance fraud in Los Angeles in 1973, a computer was used to model the company and determine the effects of the sale of large numbers of insurance policies. The modeling resulted in the creation of 64,000 fake insurance policies in computer-readable form that were then introduced into the real system and subsequently resold as valid policies to reinsuring companies.

The use of a computer for simulation, modeling, and data communications normally requires extensive amounts of computer time and computer program development. Investigation of possible fraudulent use should include a search for significant amounts of computer services used by the suspects. Their recent business activities, as well as the customer lists of locally available commercial time-sharing and service bureau companies, can be investigated. If inappropriate use of the victim's computer is suspected, logs may show unexplained amounts of computer usage.

Usually a programmer with expertise in simulation and modeling or communications would be required to develop the application needed. In some cases, however, the computer programmers had no knowledge that their work was being used for fraudulent purposes. Table 16 lists the potential perpetrators, methods of detection, and kinds of evidence in simulation and modeling techniques.

Table 16

DETECTION OF SIMULATION AND MODELING TECHNIQUES

Potential Perpetrators	Methods of Detection	Evidence
Computer application programmers	Investigation of possible computer usage by suspects	Computer programs
Simulation and modeling experts	Identification of equipment	Computer and communications equipment and their content
Managers in positions to engage in large, complex embezzlement		Computer program documentation
Criminal organizations		Computer input
		Computer-produced reports
		Computer and data communications usage logs and journals

SECTION III: Experts and Suspects

Computer crimes deal with people to a far greater degree than they deal with technology. Only people, and not computers, perpetrate, witness, or are the ultimate victims of those crimes. Therefore, investigators and prosecutors need to know more about the people and their functions in electronic data processing (EDP) than about the computer technology. Technical assistance can be obtained from experts. Because most reported crimes deal with mainframe computer systems in large organizations, this section emphasizes those computers rather than personal computers, which are generally familiar to criminal justice personnel anyway.

This section is divided into two parts. The first part discusses who can provide technical assistance and the roles of each expert in using computers. In particular, the usefulness of computer security specialists and EDP auditors is emphasized[19]. Detailed descriptions of 17 occupations, including the associated skills, knowledge, computer access, and potential crime threats, are provided in Appendix D. The second part discusses computer crime suspects. The vulnerabilities of computer systems to crime by people in specific occupations are emphasized. Characteristics of known computer criminals and aids for interviewing suspects are included.

A. Technical Assistance

Use of expert testimony is now almost standard practice in certain complicated criminal and civil cases. Experts provide important assistance by explaining difficult issues in terms that the fact finder and the attorneys can understand.

Expert testimony, however, has permissible and impermissible aspects. The permissible scope of opinion is defined under the Federal Rules of Evidence and equivalent rules for other jurisdictions. Under these rules, an expert may testify on an issue if two tests are met. First, the witness' specialized knowledge must be of assistance to the triers of fact in understanding the evidence or in determining factual issues. Second, the witness must qualify as an expert by virtue of his or her "knowledge, skill, experiences, training, or education"[20].

Computer-generated evidence, which will usually undergo legal challenges, requires expert testimony support. A problem arises when investigators think they can bring in any witness from the victimized company to testify that "these are business records." Witnesses need to know what they are talking about and be able to show that the method of generating the evidence is valid.

When deciding among several experts available to give testimony, the investigator should check for certain characteristics: sufficient professional experience, familiarity with cross examination, and a professional demeanor. Specific questions to ask potential experts include the following:

Experience—Experts with wide experience and knowledge are needed. Computer technologists usually have little or no experience as expert witnesses. They must be carefully trained and prepared for the realities of court testimony in advance, almost forced to answer in as few words as possible. The questions must therefore be well formulated so as to elicit brief answers. Experts should help in formulating the questions as well as the answers. How long have they been involved with this specialty? Have they testified on this particular subject before? Have they practiced in this particular subject matter, or is their knowledge more theoretical? Do they regularly act as expert witnesses?

Courtroom Knowledge—How the experts respond to the court proceedings can significantly affect the outcome of a case. Are the experts aware of what questions the attorneys may raise about their experience level? Can the experts limit testimony to the specific questions asked?

Courtroom Demeanor—Juries may view dull witnesses as appropriately professional, but often they will miss important information when such witnesses speak. Are the experts too dull or too lively so that their testimony is affected by their method of communications? Do the experts appear professional?

Sources for obtaining experts include the victim's technical staff, the manufacturer of the data processing system involved, other organizations that use identical hardware and the same or similar software, local universities, computer technology and security consulting services, and service bureaus having similar equipment. Because of the close relationships among technologists, the selected experts should not be associated with the suspects in any way. The experts must also be warned to keep their assistance a secret, especially among their professional associates.

When talking with computer people, the investigator or deputy district attorney (DDA) should ask for an explanation of unfamiliar and imprecise words. A glossary of terms, like the one provided in this manual, is most useful in this regard, although consensus on the meanings of many

technical terms and jargon in the computer field is rare. Despite the precise nature of the technology, computer experts are often not concerned with the preciseness of the technical terms they use, which can create serious problems in testimony.

Information about the wide range of distinct types of people and organizations encountered during computer crime investigations can be very helpful to investigators and prosecutors. The following subsections distinguish among computer technologists who specialize in electronics, programming, and operations, as well as among data providers, users, systems analysts, and programmers who specialize in scientific/engineering information and business applications. The organizations include those that use computers to conduct their business or services; those that manufacture computers, computer programs, and supplies; and those that provide computer services as a business. In addition, computer security specialists and auditors who can be of great assistance are described.

1. Electronics and Programming Experts and Witnesses

Some computer technologists are skilled in developing electronic circuitry in computers but know little about developing a major computer program; others are expert programmers but know little about the electronic aspects of the computers they use. An investigator should be aware of these differences when selecting experts and witnesses to supply information. Prosecutors experienced in questioning technologists strongly advise interviewers to insist on understanding all concepts and terminology used. The first questions should always determine the area and degree of competence:

(1) What technical education do you have, and what are the most recent courses you have taken?

(2) What professional organizations do you belong to?

(3) Are you certified by any recognized certifying organization?

(4) What is your experience in testifying or in assisting in litigation?

(5) What is your work experience by employer, job title, and job responsibility?

(6) What is the largest or most complex computer program you have written or maintained, in what language, for what purpose, on what computer, and when?

(7) What computers, communications facilities, and terminals have you worked with?

(8) What electronic components have you designed, developed, or serviced and when?

(9) Do you have sufficient experience and knowledge to answer questions concerning _____?

Interviewers must determine the individual's knowledge of and experience with the specific equipment or programming language of concern. Some technologists are familiar with one manufacturer's equipment or programming conventions but totally unable to answer questions about products of another company. For example, employment advertisements for programmers frequently specify the type and manufacturer of equipment or programming language to be used. Furthermore, a programmer experienced with one version of FORTRAN may not be knowledgeable about another version of FORTRAN.

Programmers in business and engineering environments are generally divided into two groups: applications programmers and systems programmers. Applications programmers develop the production applications that perform the business or engineering functions requested by users and designed by systems analysts. Systems programmers write and maintain the programs that control the operations of a computer system, such as managing data storage, scheduling and running applications runs, and controlling communications and systems resources. Organizations generally have more applications programmers than systems programmers. The applications programmers may be distributed among user departments, or they may be centrally organized as a service group within the data processing or information systems organization. Systems programmers are found mostly in the organization that operates the computers and in the communications group.

Investigators should assume that computer technologists are sufficiently knowledgeable about the details of a particular computer system or programming language only if they have recent, significant, and direct experience with it. Some computer facilities have a one-of-a-kind computer operating system, computer system configuration, or programming language for which only a few, highly specialized technologists may be qualified to answer questions. In some cases, application programs are still being used that were developed years ago on older generations of computers and that nobody is acquainted with in sufficient detail to answer detailed questions. Only the vendor's staff may understand the application programs and computers that are purchased or leased for use, particularly where vendor maintenance is included in the contract.

2. Systems Analysts

Systems analysts, who may not even be in computer service departments or may only be indirectly associated with computers, are also important in computer crime investigation and prosecution. They identify and develop system requirements, specifications, and design activities; in their degree of technical expertise, they fall between computer

users on one hand and programmers on the other. They tend to be specialized in certain types of applications and have backgrounds in either engineering disciplines or business functions but usually not both. They frequently have programming experience but are considered to be generally more senior than programmers. Some organizations have technologists called programmer analysts who tend to be more senior programmers specializing in applications but performing systems analysis as well as program design and development.

Systems analysts may be valuable sources of information for investigators, primarily because analysts usually are independent from yet thoroughly understand the function and activities of both the users and programmers. Because their primary function is to translate business requirements into instructions from which the programmers write programs, systems analysts can often better explain application program functions than programmers.

3. Computer Scientists

More highly trained computer technologists are likely to be proficient in both electronics and programming; they usually have advanced degrees in computer science. These people also tend to be oriented towards science, mathematics, or engineering rather than business applications. Prosecutors should be aware, however, that high degrees of specialization may tend to limit the computer scientists' knowledge of production business systems.

4. Computer and Network Operators

Computer and communications network operations staffs normally consist of high school graduates with some trade school training. They frequently aspire to become programmers, and some may be part-time college students. Except for those learning to become programmers, their knowledge and skills are limited to operating equipment and following directions contained in computer and communications operating system and operations manuals. Computer operators usually understand the external characteristics of production jobs regarding run time, frequency of errors, backup copying of data, moving programs from test to production status, and use of computer media such as tapes, disks, and paper forms. They are also familiar with computer system performance reports, journals, exception reports, accounting data, and console logs.

Operations personnel are usually responsible for ensuring that data can be recovered from locally stored backup media, media in libraries, and media transported to off-site data backup facilities. If an investigator is searching for old or possibly erased data, operators may sometimes know where backup or archived copies may be found.

Network or communications operators are skilled in preserving, routing, and rerouting data (and sometimes voice) communications links among host computers, servers, data switches, and user computers or terminals. They also monitor and preserve line quality. They usually possess monitoring equipment and connections to eavesdrop or record on any lines in use. Requests for connection to computers from dial-in lines also are received by network operators.

Operators are aware of the normal flow of production operations, including the sequence of jobs and systems resources (hardware, software, and media) used for each job and backup for recovery and restart purposes. Due to the routine nature of their job, they are highly sensitive to disruptions of the normal flow that may not appear in audit trails, and are thus a good source for identifying unusual activity in a data center. They are less useful for cases involving stand-alone microcomputer usage.

5. Data Entry Personnel

Data entry personnel can be divided into two general classifications: those in business systems and those in engineering and scientific programs. Business systems data entry personnel are usually high school graduates—clerical people with relatively little training. Engineering and scientific data providers tend to have more training in engineering and scientific subjects. They often are college students; they sometimes know considerably more than necessary about the computer applications for which they are supplying data.

Large numbers of clerical people work to produce data processed on computer systems. These people tend to be less familiar with computer technology and rarely get near a mainframe computer. They perform their data entry from remote data source locations not usually in the data center that processes the information, yet their input work starts the whole process of computer production runs. For example, retail use of real-time, point-of-sale terminal systems have converted sales clerks, ticket agents, tellers, loan officers, checkout stand clerks, service operators, and others into direct data entry personnel. Usually, processes unknown to these people result in computer output reports that are often returned to many of the data entry locations, thus closing the processing loop. Some of these people view computer technology as threatening; others see computer technology as a great aid in freeing them from tedious work.

Data entry personnel sometimes learn from experience the vulnerabilities of the computer systems they feed. Although they could engage in numerous kinds of fraud (e.g., false data entry) because they often handle assets, they are fre-

quently unaware of both the details of and controls built into computer production programs. A well-designed business data processing system would have extensive controls to detect deviations from normal activities such as duplicate billing or payments that might indicate data entry error or fraud. Unfortunately, most business systems fall short of having effective detection controls. As business systems controls develop and mature, source entry fraud is expected to decline.

For example, additional information on the activities of data entry personnel may be available from automated data entry performance monitoring applications. These applications track such entry operator performance parameters as speed and accuracy of data entry, and times and types of activity. This information can establish a baseline of average data entry activity of a specific individual. In well-designed and operated systems, each data entry person is uniquely identified by a user ID and secret password or token (key device) so that complete audit trails can be maintained. Separation of duties can often be enforced by limiting each person's allowable actions or requiring dual authorization. Audit logs such as transaction tapes in terminals and data log files in host computers can be used to identify data entry activity.

6. Mainframe Computer Users

Computer users are business- or engineering-oriented managers and staff who are responsible for accomplishing tasks for which mainframe computers are used. These people may not understand computer technology, but they work with systems analysts and programmers who translate the users' needs into computer production systems.

Business users are usually people with middle to higher level business responsibilities. Included in this expanding user category are payroll, accounts receivable, and accounts payable managers; accountants; investment analysts; production controllers; economists; and auditors. Business users tend to require large, ongoing computer production systems that need periodic production runs, online updating of large files of data, and storage of data for future production. Such systems are usually input/output bound; that is, the time required for computer processing is mostly the time for inputting data and producing reports.

The engineering/scientific users, systems analysts, and programmers are generally engineers and scientists with extensive knowledge of the particular subjects in which they are developing systems. These users include chemical, mechanical, and electrical engineers, as well as biologists, physicists, chemists, and physicians. Engineering/scientific users tend to require computer programs that are run to solve specific problems but that are no longer needed until similar problems require solution. These computer programs tend to be computation bound; that is, the production time depends on the computations performed by the computer and not the time for input and output. I/O bound exceptions to this situation include process control systems, engineering/scientific problems that require massive amounts of input data, huge input-output bound computer production runs, and large amounts of output reports. However, large production systems often tend to have a relatively short life because the solutions to problems are found, or they are replaced with new, improved computer production systems.

With the advent of departmental and end-user computing, users may be their own systems analyst and programmer, with their own production system and responsibility for security and backup. The system may be stand alone, or it may connect with other mainframe, mini- or microcomputers via one or more networks. During normal operations, users may access several different computer systems simultaneously, uploading or downloading production data bases to and from their own production system.

7. Personal Computer Users

Numerous products and applications have developed around the microcomputer and portable laptop computers. Microcomputers are small, desk-top computers that are as powerful as the computers that occupied entire rooms a few years ago. The market for these microcomputers is large, and numerous retail stores specialize in them. They are widely used throughout all levels of business and government organizations, from executives to mailroom clerks. They perform almost every type of function performed by mainframe computers and have in many cases replaced larger computer systems. To an increasing degree, these microcomputers are connected to mainframe and minicomputers, other microcomputers, and local and wide area networks.

The growth of the distributed processing concept has created a network environment where access to larger computer systems by microcomputer and connecting communication line is the rule rather than the exception. This open environment has given rise over the past few years to malicious hackers, who use microcomputers and networks to browse through any computer system they find in the network. Criminals may also use microcomputers to commit fraud. Expert assistance in recovering electronic evidence should be sought to preclude its loss. Such assistance is available from computer retail stores selling identical hardware and software, equipment manufacturers, and independent microcomputer consultants. Using hackers as experts can be dangerous because of their loyalty to their culture and their immaturity.

Microcomputers have become pervasive in small business

and professional offices. An offshoot of this microcomputer technology is word processing and desk-top publishing, for which microcomputers form the basis for the typing, editing, page makeup, and production of documents including letters, manuals, reports, and books.

Users mostly buy application programs for personal computers from computer retail stores and mail order houses. If a microcomputer is involved in an alleged crime, the investigator or prosecutor could seek technical advice from any of the many retail stores that sell the equipment and program products. The advice, however, should be sought from an individual familiar with the particular microcomputer and application because of the high degree of specialization in this field.

8. Information Systems Users and Developers

As the cost of storing large amounts of data in easily accessible computer media decreases, increasing numbers of information storage and retrieval systems are being developed. Examples are library index systems; law retrieval systems such as Lexis and Westlaw; and parts inventory in large warehousing applications. The users are the receivers of the information storage and retrieval services. Systems analysts and computer programmers who develop these services specialize in data base management systems (DBMSs).

One individual, the data base manager, is responsible for the overall administration of large files or data bases of information. His or her job is to ensure the effective use, expansion, and integrity of large data bases.

Rapidly increasing demand for timely access to these data bases has led to the widespread development of the management information system (MIS), a storage and retrieval data base application. A MIS usually consists of files of various kinds of information and a set of applications that processes and analyzes operational information; it then reduces the information to detailed and summary reports that are made available to the organization's management hierarchy. Frequently these managers access the MIS through on-line remote terminals or microcomputers on local area networks.

Crimes associated with DBMS and MIS applications tend to be sabotage, espionage, and highly sophisticated frauds involving information more than money. The technology associated with large DBMS and MIS applications is highly complex. Investigators and prosecutors are well advised to seek expert advice if they must deal with this technology.

9. Computer-Related Organizations

Investigators and prosecutors need to understand and anticipate the different kinds of organizations with which they may interact. Four major categories of organization are important:

- Those that use computers to conduct their business or services.
- Those that manufacture computers, peripheral equipment, computer programs, and computer-related supplies.
- Those that provide computer services as a business.
- Those that provide communications services.

a. Computer User Organizations

Top managers of computer-using organizations frequently do not understand the technology, abrogating significant responsibility to data processing managers. These organizations either have and operate their own computers, have their own computers and contract to a facilities management company to operate them, or do not have computers but use outside computer service companies to do their processing. Many organizations also engage in various combinations of these methods.

Some large organizations that use computers for both applications and normal business functions have separate computer centers: one type for business data processing and one type for engineering and scientific data processing. Rarely are they combined into a single computer system because of the differences in the systems as well as the personnel needed to operate and program them. Where they are combined in one computer center, conflict often erupts between these two different groups of people.

The proliferation of low-cost, high-performance minicomputers, microcomputers, and time-sharing services has moved computing activity down to the specific departments and users that need computer services. A large business or government organization may have one or more large central computer centers, ten or even 100 minicomputers in individual departments, thousands of personal computers, and several hundred people using outside commercial time-sharing services through computer terminals and telephone circuits.

Contention in the computer field continues over the advantages and disadvantages of large centralized computer facilities serving an entire organization versus various configurations of distributed computing. Decentralized organizations with extensive departmental data processing frequently must contend with inconsistent procedures and departmental policies. Other large businesses, however, are centralizing what was once a widely distributed array of computers. Computer technology can now economically support both of these types of configurations as well as any combination.

Another trend resulting from the explosive growth of microcomputers is end-user computing, where the users themselves process their information independently of mainframe and departmental computer systems. The com-

pany provides the users with computers, software, and access to data bases through networks. Typically, such companies also have an end-user computing unit, which supports the end-users and is a good source of technical information on end-user data processing.

b. Manufacturing Organizations

Organizations that manufacture computers, peripheral equipment, computer programs, and supplies also may be sources of information for the prosecutor or investigator. Because these organizations tend to be large, complex businesses, they are frequently users of their own products; hence, they are similar to the organizations discussed above. In obtaining information from manufacturing organizations, investigators and prosecutors need to find individuals with sufficient expertise to provide adequate information. The public relations office, security department, or internal audit department may be helpful in locating qualified individuals. Many businesses eagerly provide information free of charge either as a public duty or out of self-interest to minimize the negative image of involvement in a computer crime.

c. Computer Service Organizations

Organizations that sell computer services tend to be very technically oriented. The basic kinds of services offered are service bureau batch services, time-sharing services, and network services. Most large service companies now offer all of these services, although hundreds of small service bureaus still pick up input from their customers, perform the computer processing, and return the output to them.

Because these companies tend to be highly competitive, they have been subject to industrial espionage and sabotage. Employees of computer services organizations are generally in high positions of trust; they have wide access to the often sensitive data of their customers. Therefore, computer service organizations tend to have more advanced security than other organizations and often emphasize security in their advertising. Usually, these organizations are very reluctant to supply information about the nature of their customer's data processing. Like banks, they try to protect their security and safety image.

These organizations sometimes specialize in certain types of data processing. Some may sell their services to provide business data processing, some may concentrate on engineering/scientific data processing, and others may offer specialized information services. These organizations also provide various amounts of systems analysis and computer programming services. An organization may provide complete services in the design, development, and production of application systems. Others may provide only the computer services, leaving it up to their customers to develop their own computer programs.

Computer service organizations are now offering more universal computer applications. If users can fit their application's needs into a preprogrammed package, they can significantly reduce the costs of computer program development. The competitive nature of these organizations has resulted in each organization providing a wider range of more sophisticated application programs than its competitors. The application programs are normally available only for use with their computer systems; they are not sold or licensed directly to the users. These programs tend to be protected as trade secrets rather than by copyright.

Finally, facilities management companies contract with organizations to run their in-house computers. This arrangement exposes the staff to complex trust relationships. The specialized companies provide off-site data backup and hot-site processing backup services that also place them in high positions of trust.

d. Communications Service Providers

Most large computer-using organizations connect their computers to various types of networks (e.g., local area networks, wide area networks, and public networks). A huge industry for data communications has developed; both the well-known general communications companies and many specialized companies provide value-added services such as computer applications, electronic mail, subscription services for data bases, and local switching at customer sites. Low-speed (200 to 1600 characters per second) and high-speed (above 50,000 characters) data communications are provided using various standard formats and transmission modes including wires, optical fibres, microwave, radio, and satellite.

Data communications have revolutionized computing and added significant vulnerabilities, mostly by exposing information to loss outside of the security perimeters of users and eliminating geographic constraints on perpetrators who traditionally had to be at the physical locations of information loss.

10. Information and Computer Security Specialists

Computer crime acts often include the violation, neutralization, bypass, or avoidance of controls and security practices that would otherwise prevent or detect the illegal act in a timely way. The computer security specialist (now also called an information or data security specialist) plays an important role in helping to protect organizations using computers.

Information and computer security is still an emerging profession. A number of universities, research institutes, computer manufacturers, and government agencies are attempting to apply analytical methods to information security and

develop the needed controls and security practices. Security is being improved to keep pace with the increasing amounts of information assets that are being stored, processed, and communicated with computers.

Prosecutors and investigators should be aware that the people responsible for the advancement of computer security are primarily computer technologists who lack industrial security or criminal justice backgrounds. They have generally treated information security as a technical subject that is amenable to technical solutions. They are only starting to understand that information security is primarily a problem with the behavior and activities of people and that a real enemy exists with malicious intent. At the same time, specialists in industrial security and people with criminal justice backgrounds have not gained sufficient technical capabilities to effectively apply their knowledge and backgrounds to computer security problems.

Information security specialists are not immune from being perpetrators of computer crime. They are in high positions of trust, and several have violated their trust to engage in crime (most notably, see cases 78313 and 88214 in Appendix C).

a. Responsibility for Security

Information security is the generic term used to identify, develop, or administer all kinds of controls and practices needed for ensuring the safe use of information technology[21]. The responsibilities for information security in a computer-using organization are usually split among various functions. Security is the direct responsibility of each manager in his or her particular area. The auditors act in a staff capacity, assisting line management by determining the effectiveness of the security in a line manager's area. The information security specialist or computer security coordinator also is responsible for assisting line managers. The security specialist usually has specific security responsibilities for administration of computer and physical access controls into computer facilities. This person is also responsible for producing the overall plans for security and the procedures for implementing them. Finally, each employee is responsible for assuring that the work is conducted in an appropriate, secure manner.

b. Security Organization

Information and computer security in most large organizations is planned, developed, and implemented within the computer services area of an organization rather than in the traditional area of the industrial security or protection department concerned with physical security throughout the organization. The reason for this segmentation is that most industrial security specialists have not yet gained sufficient capabilities in computer technology to deal with the complexity of computer security. Yet, focusing information and computer security in the computer services department often results in suboptimization of security because the function does not have sufficient authorization and industrial security expertise to impose security among computer service users in other parts of the organization.

The information and computer security specialist, a new occupation formed within the last 10 years, is not yet a well-established occupation. Requirements have not been generally agreed upon, and no school offers a course of study that prepares an individual for this occupation. Computer security specialists generally come from technical jobs, such as computer programming, systems analysis, or computer operations management within the computer field. Only the very largest computer organizations have established computer security units with one or more full-time computer security specialists or coordinators. More often, individuals in lower management or technologists from a standards, procedures, and training function are appointed to coordinate computer security on a part-time basis as only one of their responsibilities. Other organizations periodically establish temporary task forces or committees to evaluate security and make recommendations to management.

11. Auditors

Both external (contracted) auditors and internal (employee) auditors are particularly helpful in economic crime investigation and prosecution. The specialization of some auditors in computer technology makes this EDP audit expertise also of value in computer crime work.

Certified Internal Auditors (CIAs) have been certified by the Institute of Internal Auditors (IIA). Certification includes subscribing to a code of ethics, holding a baccalaureate degree or equivalent work experience, and passing an examination based on a "Common Body of Knowledge for Internal Auditors"[22]. The CIA rating was established to promote and increase the professional standing of internal auditors but is not a requirement for being an internal auditor.

The issues of detecting and investigating fraud and other irregularities have varied over the years and from one organization to another. Some organizations do not charter their internal audit function with responsibility for detecting fraud, justifying this decision on a cost/benefit basis. Other organizations view the internal audit function as both detecting fraud and acting as a deterrent to fraud. The consideration for fraud detection is directly addressed in the IIA's "Standards for the Professional Practice of Internal Auditing"[23]. The reference is not limited to any one area such as EDP, but is a general standard dealing with due professional care.

> ...in exercising due professional care, internal auditors should be alert to the possibility of intentional wrongdoing, errors and omissions, inefficiency, waste, ineffectiveness, and conflicts of interest. They should also be alert to those conditions and activities where irregularities are most likely to occur. In addition, they should identify inadequate controls and recommend improvements to promote compliance with acceptable procedures and practices.
>
> Due care implies reasonable care and competence, not infallibility or extraordinary performance. Due care requires the auditor to conduct examinations and verifications to a reasonable extent, but does not require detailed audits of all transactions. Accordingly, the internal auditor cannot give absolute assurance that noncompliance or irregularities do exist. Nevertheless, the possibility of material irregularities or noncompliance should be considered whenever the internal auditor undertakes an internal auditing assignment.
>
> When an internal auditor suspects wrongdoing, the appropriate authorities within the organization should be informed. The internal auditor should recommend whatever investigation is considered necessary in the circumstances. Thereafter, the auditor should follow up to see that the internal auditing department's responsibilities have been met.

The Bank Administration Institute (BAI), also concerned with standards of internal auditing, has issued a statement on the internal auditors' responsibility for detecting fraud. The statement appears in the BAI's "Statement of Principle and Standards for Internal Auditing in the Banking Industry"[24].

> Audit proficiency includes the ability to evaluate fraud exposures. Sufficient information is available in the literature on auditing concerning how frauds may be committed in banking. The auditor should be familiar with that literature.
>
> The systems of control and not the internal audit function provide the primary assurance against fraud. Internal auditors, however, must evaluate the capability of the systems to achieve that end. When in doubt the auditor should consider applying additional procedures to determine if fraud has actually occurred.
>
> In fixing the internal auditor's responsibility for detecting fraud, it should be recognized that the internal auditor cannot be responsible for detecting irregular transactions for which there is no record, e.g., an unrecorded receipt of cash from a source for which there is no evidence of accountability; an isolated transaction that does not recur, e.g., a single fraudulent loan; or irregularities that are well concealed by collusion. However, in the usual course of the audit cycle, the internal auditor should detect irregularities that significantly affect the financial statements, repeatedly follow a suspicious pattern of occurrence, or those that can be detected by a reasonable audit sampling. Internal auditors must also accept responsibility for those irregularities that result from their failure to report known weaknesses in the systems of control.
>
> In judging the preventive capacity of the control systems and the internal auditor's responsibility, the principle of relative risk should not be ignored, namely, costs must be balanced against intended benefit.

The EDP auditor can be an excellent source of information. Because the function is based on (or usually is a part of) internal audit, important professional standards and principles dictate how work is performed. Specific information on controls, weakness in security, recommendations for strengthening controls, and general information on elements of the EDP environment should be readily available from them. In addition, the EDP auditor often has computer tools specifically designed to assist investigators in reviewing, testing, and evaluating computerized records and computer systems. (Appendix E describes a number of the most relevant EDP audit tools.) Some EDP auditors may even be experienced investigators of computer fraud or abuse.

Topics that EDP auditors should be familiar with include:

- Basic topics: introduction to data processing, computer hardware overview, computer programming overview, computer documentation overview, introduction to data processing application controls, and introduction to general data processing controls.
- Advanced topics: on-line systems controls, data communication controls, continuous operation controls, storage media/device controls, audit trace considerations, and special audit software.

EDP auditors use numerous tools and techniques to audit the computer environment. The tools and techniques can be classified by the function that they perform:

- Auditing systems development and change control: code comparison and system acceptance and control group.
- Computer application control testing: test data method, basecase system evaluation, integrated test facility, and parallel simulation.
- Selecting and monitoring transactions for compliance, testing, and data verification: transaction

selection, embedded audit data collection, and extended records.

- Data verification: generalized audit computer program.
- Analysis of computer programs: snapshot, tracing, mapping, and control flowcharting.
- Auditing computer service center: job accounting data analysis.

The most widely used tool is the generalized audit computer program package. The other tools and techniques that have been used the most are test data method, transaction selection, and control flowcharting. Brief descriptions of these EDP audit tools and techniques and a list of computer-related occupations of possible suspects (from Appendix D) that could be affected by the use of the tools are given in Appendix E[25].

The following major strong points of EDP auditors make them valuable in a computer crime investigation:

- Level of confidence. Because of the nature of their profession, auditors are highly respected as analysts and evaluators; the standards, principles, and codes of ethics that dictate how auditors conduct their work are well established; to a degree, auditors have a responsibility to their profession as well as to their employer.
- Technical expertise. With proper training and experience, EDP auditors provide a high level of EDP technical knowledge, both for the data processing profession in general and the specific computer environment within their organizations.
- Tools and techniques. Because EDP auditors must regularly use EDP audit tools and techniques, they are often available for testing and investigation; the EDP auditor should have some of these tools ready for immediate use (especially a generalized audit computer program package that can be used for retrieving and analyzing computerized records). However, the admissibility of evidential data obtained using these tools as an ordinary business practice is doubtful.
- Independence. Because auditors have no direct responsibility for nor authority over any of the activities that they review, they have a broad mandate, and they report to top management. Their independence is well established, a critical factor in any investigation.

The following major weak points of EDP audit must also be considered in a computer crime investigation, however:

- Relationship in organization. Because audits are evaluations of the organization, they often cause the EDP audit and audited groups to disagree; this conflict can result in an adversarial relationship that may compromise cooperation.
- Inexperience of profession. Because of the relative newness of the EDP audit specialization in contrast to the general field of audit, generally accepted EDP audit principles, standards, guidelines, and tools and techniques are still developing.
- Training. Even with formal education and certification programs, the level of EDP auditor expertise varies widely; some have excellent EDP and audit backgrounds, others are much stronger in one area than the other, and some have entered the profession with a very low level of EDP audit knowledge.

a. Audit Organization

Most large organizations, both in the private and public sector, have internal audit departments. These departments provide an independent appraisal of operations as a service to senior management (independent from a department or functional viewpoint, but still part of the same organization). They function as a managerial control by measuring and evaluating the effectiveness of other internal controls. Although an internal audit function is not required, the Securities and Exchange Commission (SEC) strongly recommends that organizations falling under the SEC Act of 1934 have such a function.

Many organizations that have significant computerized systems also have an EDP audit function. This function may be a separate department, part of internal audit, or part of some other department. The EDP audit function also serves as an independent tool for senior management to evaluate internal controls in the EDP environment.

The need for EDP auditing has come from a change in the way the computer stores and processes data rather than from a change in accounting theory or auditing principles. New tools, techniques, methods, and auditor expertise are required.

b. External Auditors

Independent certified public accounting firms audit corporations and certify the accuracy of corporate financial information (for example, the statement in a company's annual report). These audits are performed under the provisions of the federal securities laws. When acting as the independent auditor of a publicly owned corporation, the external auditor has public responsibilities and must satisfy requirements of the federal and state governments regarding performance of those responsibilities. The objective of the independent auditors' examination of financial statements is the expression of an opinion on the fairness with which they present the financial position, results of operations, and change in financial position in conformity with generally accepted accounting principles.

CPAs (certified public accountants), certified by state examining boards as having met stringent qualifying requirements to practice accounting, may serve as independent auditors for publicly owned corporations. Noncertified accountants may engage in some of the audit work, but a CPA is required to direct the effort and to sign the opinion.

The American Institute of Certified Public Accountants (AICPA) is the national association that guides and directs the auditing profession. Various AICPA committees are chartered to issue pronouncements and rules on auditing matters; for example, "Statement on Auditing Standards Number 3, The Effects of EDP on the Auditors' Study and Evaluation of Internal Control"[26]. In addition, a code of professional ethics supports the standards and provides a basis for their enforcement.

Although external auditing does not include internal controls per se (e.g., controls involved with data processing), a number of CPA firms have developed audit tools to assist in EDP auditing. The major tool, the generalized audit computer program package, is used to retrieve and analyze data stored in computer files.

From an EDP perspective, external auditors typically do not perform a detailed review of the full computer environment—the financial attestation does not require that type of effort. Nonetheless, they usually have staff with EDP expertise and use them as needed, typically for either helping to extract computerized financial records or for management consulting on special projects (other than the financial audit function).

CPAs normally produce two reports, the opinion letter and a management letter. The opinion letter is a short statement of the scope and date of the audit, an opinion of the accuracy and fairness of the financial statement, any exceptions, and whether the financial statements are presented in accordance with generally accepted accounting principles that have been consistently observed over the preceding periods. The management letter includes findings regarding weak or missing controls and recommendations for corrective action. In addition to producing these formal reports, external auditors have well-defined standards of fieldwork that include the compilation of sufficient evidential matter (in work papers) to support the rendered opinion.

The consideration for fraud responsibility is precisely defined in the AICPA's "Codification of Auditing Standards and Procedures"[27]. The reference is not limited to any one area such as EDP but is an overall position:

> . . . opinion on financial statements is not primarily or especially designed, and cannot be relied upon, to disclose defalcations and other similar irregularities, although their discovery may result. . . . The responsibility of an independent auditor for failure to detect fraud (which responsibility differs as to clients and others) arises only when such failure clearly results from failure to comply with generally accepted auditing standards. . . . The subsequent discovery that fraud existed during the period covered by the independent auditor's examination does not of itself indicate negligence on his part. He is not an insurer or guarantor; if his examination was made with due professional skill and care in accordance with generally accepted auditing standards, he has fulfilled all of the obligations implicit in his undertaking.

However, this fraud audit responsibility will be increased in 1989.

B. Characterizing Suspects

This section provides aids for identifying and dealing with suspects. The people who represent potential threats based on their skills, knowledge, and access to resources are identified below. The results would not necessarily be the same in every victimized organization because of differing practices and safeguards. In a computer environment, four basic sources of potential perpetrators can be established:

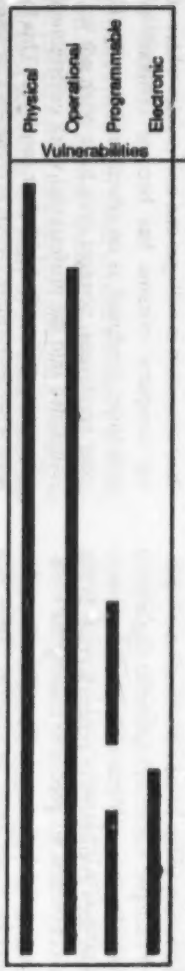
- People with physical access to assets and the capabilities to perform physical acts
- People with any kind of access and operational capabilities
- People with any kind of access and programming capabilities
- People with any kind of access and electronic engineering capabilities.

This classification suggests an approach to identifying these people in terms of their occupations. The suspects may include not only employees and individuals under contract, but also managers and any outsiders who have sufficient skills, knowledge, access, and resources to represent potential threats to computer systems, networks, and facilities.

Table 17 presents the results of a vulnerability analysis associated with acts causing loss of integrity, confidentiality, and availability against eight forms of assets and general types of safeguards for each occupation. An entry on the line of a particular occupation in the column "Internal Data/Confidentiality," for example, indicates that an individual could cause a loss of confidentiality of data internal to the system. A blank entry denotes no effect. For all

Table 17

OCCUPATIONAL VULNERABILITY ANALYSIS



Occupations	Vulnerable Assets by Acts																							
	Internal Data			Internal Application Programs			Internal System Programs			External Data			External Application Programs			External System Programs			Computer Equipment & Supplies		System & Network Services			
	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	I	A		
Media librarian											X	X		X	X		X	X		X				
User media librarian											X	X		X	X					X				
User trans. & data entry operator	X	X	X		X	X				X	X	X		X	X					X				
Computer operator	X	X	X		X	X		X	X	X	X	X								X	X	X		
Peripheral equipment operator											X	X		X	X		X	X		X				
Job set-up clerk											X	X		X	X					X		X		
Data entry & update clerk	X	X	X		X	X		X	X	X	X	X		X	X		X	X		X				
Facilities engineer																			X	X	X			
Operations manager	X	X	X		X	X		X	X	X	X	X		X	X		X	X		X	X	X		
Data base administrator	X	X	X							X	X	X								X				
System programmer		X	X		X	X	X	X	X							X	X	X		X	X	X		
Applications programmer	X	X	X	X	X	X							X	X	X					X				
User programmer	X	X	X	X	X	X							X	X	X					X				
Programming manager	X	X	X	X	X	X							X	X	X					X				
Communication engineer/operator		X	X																X	X				
Terminal engineer																			X	X				
Computer system engineer							X	X	X										X	X				
Security officer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		
EDP auditor	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		

Acts

I — Violation of integrity

A — Violation of availability and use

C — Violation of confidentiality

acts, it is assumed that perpetrators profit or could profit from their acts and that victims experience or could experience losses from the acts.

As defined for this table, loss of integrity involves changes in the content or intrinsic condition of objects or services that could result in criminal charges, including fraud, embezzlement, sabotage, or vandalism. Loss of confidentiality entails the loss of secrecy or privacy that could result in criminal charges, including theft of trade secrets, copyright or patent violation, or espionage. Loss of availability means interfering with or preventing objects or services from being used when, where, and how they were supposed to be. Criminal charges could include larceny (theft or burglary), robbery, sabotage, fraud, embezzlement, or vandalism. All three types of information loss could result in more general charges such as bribery, antitrust violations, racketeering, insider trading, and conspiracy.

Assets in the form of data, application programs, and system programs are designated as internal to a computer system when the central processor has continuous access to them from any attached storage device. Assets are considered external to a computer system when they are in human-readable or computer-readable form and where computer personnel have manual, direct access to them. Computer equipment, facilities, supplies, and services complete the range of types of assets.

The matrix entries in Table 17 reflect an environment in which the usual safeguards and controls have been installed in idealized, totally effective ways. Different matrix entries might be assigned for a specific computer environment based on the actual safeguards in place. For example, whenever the access and functioning of an individual can be limited, the matrix assumes that this occurs. One reason that the application programmer and the user programmer are assigned a limited rather than a great exposure level is that these individuals are assumed to communicate with the system through programmer terminals or intermediaries. They never have access to current production, and independent computer program verification occurs before their products are put into production. Similarly, the computer system engineer is assumed to be forbidden from working on a computer system when any production data or application programs are present.

Occasional ambiguity exists in the classification of a particular act. For example, a system programmer might cause an integrity loss of a system program internal to the system and successfully deny availability of system service. In this situation, the convention adopted is to classify the violation in the category that had to occur first. Therefore, this example would be classified as an integrity rather than availability loss.

Note that occupations are described in generic and idealized form in terms of job function, skills, knowledge, and access. In practice, the skills, knowledge, and access of personnel do not exactly match these descriptions of their occupations. For example, a computer operator (including an end-user) who has programming skill, knowledge, and access in addition to operator capabilities would be classified as a programmer as well as a computer operator in this report. If a person functions in both capacities, then the two occupations presented here would be combined in depicting the individual as a source of exposure to loss, and all vulnerabilities and safeguards in both descriptions apply to the individual.

Collusion of two or more individuals is not considered. Each individual is assumed to perform a single act alone with a single asset. In actual experience, a loss often results from sequences of parallel independent and dependent acts involving several assets in several forms. Collusion seems to occur frequently in computer crime cases, suggesting that investigators should always strongly suspect that more than one perpetrator is involved. Appendix D describes 17 occupations, including function, knowledge, access, vulnerabilities, risk level, general safeguards, and conclusions.

1. Suspects' Characteristics and Circumstances Based on Experience

Suspects may be identified on the basis of characteristics of known computer crime perpetrators who have been interviewed in computer abuse studies[25]. According to the results of interviews with a small group of 100 perpetrators, organizations will be more vulnerable to people with the characteristics described below and where these circumstances are present. Experienced investigators may note that these characteristics are similar to those of the modern-day, amateur, white-collar criminal. Moreover, these characteristics cannot be considered conclusive or complete because they are identified from such a small number of interviews. Nevertheless, the documentation of them here should provide the investigator with important clues to computer crime suspects.

a. Age

Anticipate that perpetrators will be young. Younger people in data processing occupations tend to have received their education in colleges and universities where attacking computer systems has become common and is sometimes condoned as an educational activity. Unlike older employees, younger ones have often not yet been assimilated into the professional work environment and may not have identified with their employer. This loyalty issue is becoming more serious as companies increase their use of temporary, contract workers in technical positions.

b. Skills and Knowledge

Anticipate that suspects could be among the most skilled and higher performing technologists. One of the greatest vulnerabilities in an organization comes from workers who are overqualified for the work that they are doing. An abundance of bright, highly motivated technologists enter the computer field and find themselves placed in routine jobs requiring low levels of skill (e.g., programmers engaged in the detailed work that leaves little room for innovation and recognition). These people become easily frustrated and look for other, possibly illegal ways of using their skills, knowledge, and energy.

c. Positions of Trust

In most cases, perpetrators performed their acts while working at their jobs. One exception was an individual who, while president of an electronics supply house, posed as a telephone company employee to order the delivery of telephone equipment through the telephone company computer system. However, even in this case, the individual had to pose as an employee to obtain the necessary information to engage in the fraud.

When investigating a potential loss, anticipate that the vulnerabilities identified will usually result in the most qualified person(s) taking advantage of them. If a crime involves computer programs, anticipate that the suspects may be the computer programmers and experienced microcomputer users who have access to and knowledge of the computer programs or through those programs to the assets found to be missing. If the vulnerability discovered is in the data entry function, then anticipate that suspects may be among the data entry clerks.

Next consider all other technical and operational functions where vulnerabilities may arise. Computer programmers are not likely to go into the foreign environment of the data entry section to engage in unauthorized technical acts, but managers can often cross organizational lines. Neither will data entry clerks be likely to attempt to modify or introduce computer programs into a computer to engage in criminal acts unless they are in collusion with others. They will most often limit their activities to their own work areas that they know best, and usually they know that particular area better than anyone else. Table 18 lists the occupations of perpetrators of computer crime and the likely victims.

Table 18

RELATIONSHIP OF PERPETRATORS' OCCUPATIONS TO LIKELY VICTIM

Perpetrators' Occupations	Victims
Teller	Bank
Accountant	Computer service
Company owner	Small manufacturing company
Time-sharing user	Time-sharing computer system
Business programmer	Small bank
Systems programmer	State, government agency
Computer operations and systems manager	Financial institutions
President of a firm	Electronics supply company
Business manager	Large manufacturer
Sales manager	Large retail service organization
Malicious hacker	Organization with dial-in telephone access to popular computers or services

d. Assistance

Perpetrators have been found to need assistance in many known computer crimes, whereas ordinary white-collar crime, embezzlement for example, involved a low degree of collusion according to a study of 271 bank frauds and embezzlements[28]. Collusion seems to occur regularly, primarily because computer crime requires more knowledge and access than one individual usually possesses. Collusion often involves a technologist who can perform the technical part of the act and another individual outside the computer system who can convert the technical act into irreversible gain. In one case, the computer programmer in a large organization wrote a computer program and executed production runs to calculate football pool betting odds for an organized crime ring operating a large number of football betting parlors. The computer programmer was being paid an additional $50 a week and did not know the ultimate purpose of the reports he was producing for his brother-in-law, an intermediary between him and the football betting conspiracy.

e. Differential Association

The differential association syndrome is the white-collar criminals' tendency to deviate in only small ways from the accepted practices of their associates[29]. This vulnerability stems from groups of people working together and mutually encouraging and stimulating one another to engage in unauthorized acts that escalate into serious crimes. The competitive nature of technologists in the computer field, and their often elitist attitudes, can result in a one-upmanship competition in performing pranks.

The 1973 Ward vs. California case involved the theft of a computer program from the memory of a competing service bureau computer over telephone lines from a batch terminal in the perpetrator's service bureau. A programmer

from the victimized firm admitted on the witness stand in the associated civil trial that it was common practice for programmers in both of the competing service bureaus to gain access to the other company's computer system to play games, investigate the level of use, or obtain the identity of customers and the type of work they were doing. This type of vulnerability makes it important for the investigator to interview the associates of possible suspects to determine the degree of differential association that could lead to information about some of the more innocent acts or pranks engaged in that might have led to the more serious alleged crime.

f. Robin Hood Syndrome

Most of the computer crime perpetrators interviewed exhibited the Robin Hood Syndrome[30]. They differentiate strongly between harming people, which is highly immoral within their standards, and harming organizations, which they condone. In addition, they rationalize that they are only harming a computer or the contents of the computer and thus not harming or causing any loss to people or organizations.

This characteristic is probably common among all types of amateur white-collar criminals and may not be unique to computer criminals. However, it may be more pronounced in this case because of the role the computer can play in strengthening the rationalization process. Interviews with computer crime perpetrators revealed that they would become quite disturbed if the interviewer even implied, let alone directly accused them of causing individually identifiable people to suffer losses. A New York City bank embezzler, who engaged in a fraud in his position as head teller, indicated that he never took more than $20,000 from any one savings account because he knew it was insured to $20,000. Thus, the loss was suffered by the insurance companies and not by his individual customers.

g. Game Playing and Hacking

The vulnerability of game playing is based on the concept that some computer technologists and users believe that using an idle computer does no harm and that they have a right to use it for personal purposes for challenging intellectual exercise. All but one of the computer crime perpetrators interviewed indicated that the attraction and challenge of thinking of their computer crime as a game played a significant part in motivating them to continue in their fraudulent activities. Computer technologists, especially hackers, tend to be the type of people who like mental challenges and complex game playing. Suspects believe that they have the right to play games in computers because they have the unique capabilities to do so (the hacker syndrome).

Hackers are defined to be compulsive, dedicated programmers intent on exploring the intricacies of computers and on attempting to make them fail. Hacking was considered to be an honorable pursuit when it began at MIT and Stanford University in the early 1970s. Most competent programmers have engaged in hacking; however, excessive zeal and intrusions into others'computers resulted in offensive activities that gave hacking an unsavory reputation. Hacking reached a peak of public attention in 1984 with the arrests of the 414 Gang in Milwaukee and the subsequent Congressional hearings on the problem. Since then, hacking has had a negative, illegal connotation, particularly in the news media. Real, law-abiding hackers describe the mostly juvenile delinquents engaged in computer intrusion and software piracy as crackers.

2. Antagonistic Personnel and Organization Relationships

The antagonistic and dependent relationship among people in different data processing functions is important for the investigator and prosecutor to know and understand. Among 669 reported cases of computer abuse[2], collusion occurred in one-half of the cases, but not between programmers and computer operators, probably because of their antagonism. Programmers often complain about computer operator's performance in running their programs. Computer operators complain about the practices of programmers that make their programs difficult to run and prone to errors.

Table 19 shows the potential antagonistic relationships among workers in different data processing functions. The information in this table can help investigators to understand the problems that one worker can have in interfacing with another worker. This diagram also implicitly shows in what ways workers in different data processing functions depend on workers in other functions.

3. Interviewing Suspects

Investigators need to fully understand the damage that a suspect employee can do in a computing facility. If an employee believes he is a suspect, he could cause great losses and destroy evidence, even after the crime has been perpetrated. Logic bombs (see Section II) that might be left inside a computer system represent another danger. Suspects should be prevented from access to sensitive systems, facilities, and computer media except under carefully controlled conditions.

Prosecutors should run a criminal background check not only on the suspects, but also on the victims. Such a check may be a standard practice in normal investigations, but it is particularly important in computer crime cases, since most employers fail to do this. Suspects are often willing to talk to investigators because they consider their activities to be legal. Sometimes, they think their act is unethical or immoral, but not criminal.

Table 19

POTENTIAL ANTAGONISTIC RELATIONSHIPS AMONG DIFFERENT WORKERS IN DATA PROCESSING FUNCTIONS

	Operators	Programmers	Media Librarians	Data Entry Clerks	Source Data Preparers	Users	Vendors' Maint. Engineers
Operators	From/To Complaints	Job failures; failure to report errors	Unrecorded removals and submissions			Job failures; failure to report errors	Misuse of equipment; failure to report errors
Programmers	Poor program design; misleading or absent instructions		Misleading or absent instructions	Poor input formats; poor instructions	Poor input formats; poor instructions	Lack of problem understanding; poor documentation	Programs; improper use of equipment
Media Librarians	Slow or incorrect media selection	Loss of media; incorrect labeling				Loss of media	Poor handling of media
Data Entry Clerks	Data errors causing reruns	Data errors unanticipated in program design; program entry errors	Loss of media assigned to them			Data entry errors causing erroneous output	Misuse of equipment
Source Data Preparers	Data errors causing reruns	Data errors and out-of-range data not anticipated in program design		Poor legibility on data forms		Data errors causing reruns and incorrect output	
Users	Inconvenient run schedule demands Poor job instructions	Unclear or absent problem specifications; inconvenient program change demands	Misleading or absent instructions	Inconvenient work schedule demands	Poor instructions; inconvenient schedule demands		
Vendors' Maint. Engineers	Inconvenient equipment maintenance schedule; equipment failures	Equipment failures		Inconvenient equipment maintenance schedule; equipment failures			

Before confronting or interviewing a suspect, an investigator should consider that some prosecutors will not accept a crime case until the victims assure them that they will see the prosecution through to the end and be willing to testify. Often, halfway through a long case, a victim decides to accept restitution and drop the prosecution. In addition, jurisdictional problems often must be settled because of the wide range of geographic constraints and freedoms in on-line computer systems. Many computer systems reside in one jurisdiction but are used from terminals in many other jurisdictions.

SECTION IV: The Computer Crime Environment

This section is designed to acquaint investigators with aspects of computer usage, data processing organizations, and the physical and operating environments of computers and data processing to help them gain the necessary insights to be effective in discovering a computer crime. Following an overview of these topics is an assessment of the current and future impact of the rapidly expanding use of data communications technology on each of these areas and on computer crime investigation. Finally, a discussion of computer system vulnerabilities is presented to help investigators understand this unique technical environment.

A. Today's Usage of Computers

1. Computer Usage in Science and Engineering

The first computers were designed and built for the solution of complex mathematical problems. ENIAC (Electronic Numerical Integrator and Calculator), developed during World War II for the computation of weapons ballistic schedules, was the first all-electronic calculator[31]. From these early beginnings computers have become the basic computation tool of almost all scientific and engineering disciplines.

Scientists are trained and experienced in the methods needed to define and solve the quantitative problems encountered in their professional fields. In many cases, these solutions have been previously developed into computer programs that are made available to the user for a fee. Scientists need enter only the variables in the form required by the computer program, and the solution is computed and returned to them. In other cases, scientists develop their own computer program for the solution of a newly encountered problem or a previously solved problem in a new or preferred way. This computer program, often considered a proprietary secret by the scientist's employer, is used for the solution of one problem or a series of similar problems.

Scientists, mathematicians, engineers, and others being trained in the quantitative disciplines today are taught to use the computer extensively as a problem-solving tool. They are usually taught when and how to use several computer programming languages. Their background typically includes undergraduate and advanced degrees in the physical, life, and social sciences and engineering.

Scientists often use a programmable calculator or a small specially designed computer for some of their problem-solving work. In other cases, they share a larger computer with other users. When a larger computer is shared, each user's computer programs and data can be isolated from all other users when necessary. The scientific user is given a unique identification and password, which is used to store private data files in the computer and subsequently to gain access to the data and/or programs. A special computer operating control program controls access to the owners' information stored in the computer. Users can access only their own private store of information.

Because of their expertise, these computer users often work without programming assistance and do their own programming or use previously developed programs. Typically, they do not need to communicate with any person in computer services to do their work. Exceptions occur when the process fails or when new kinds of issues arise.

2. Computer Usage in Organizations

The major organizations of our society—the businesses, government agencies, and other bodies—do much of the work and employ most of the work force. Hence, they account for the largest number of computer users today. Unlike engineers and scientists, however, production or operational members of an organization depend on others for information and procedures that are essential to the conduct of their work. Others in turn depend on these workers. Seats cannot be reserved on a flight until someone, probably far removed from the reservation agent, has scheduled the flight and entered it into the computer. Reservations cannot be confirmed unless all reservations previously made are known to be entered.

The organization is typically concerned with efficiently processing large amounts of information. The bank, the retail merchant, the telephone company, the police department, the airline, and the census bureau—all depend on effective information processing. The computer has become the dominant means for meeting the diverse information processing needs for these and many other kinds of organizations. This need to process large amounts of information through a computer effectively and efficiently has fostered the development and growth of the information processing specialist.

The specialized computer science curricula so prevalent in colleges and universities today were developed as a direct response to the need to train and develop candidates for information processing positions in business and other organizations. Practically all persons hired for government and industry positions receive a minimum level of computer-related instruction in college or company-sponsored courses. Although these classes are usually sufficient to acquaint them with the use of computers, they

do not offer the advanced information processing techniques contained in the computer science curriculum.

Because of the important role of computers, particularly in business and industry, departments that specialize in computers and information systems have been created. The information systems department has the responsibility for developing effective and efficient computer systems to meet the organization's information processing needs and for managing and operating its computing resources. This department supplies information processing services to other departments that need them to perform their work.

The organizational user of computer services interacts with the information systems department in two primary ways: with staff in the departmental section that operates the computer and performs the information processing on matters concerning ongoing production or operational computer systems; and with people in the section that develops and maintains the production computer systems, including systems designers and programmers to ensure that new and modified systems satisfy user requirements.

Virtually all large organizations use information services to process their payroll; to compute the gross and net pay and issue checks or make deposits; to compute and record the related information, such as payments due to governmental entities, credit unions, and so on; and to supply the information necessary for compliance with the various laws and agreements governing salaries and wages. The payroll example is used here to illustrate the respective roles of the information systems department and the computer services user.

The payroll department typically collects time records or other proof of wages due, checks to make sure they are properly signed, and develops a batch control such as number of records and an arithmetic total of the total hours shown. If required, the time records then go to computer operations where data entry operators record the information from the time cards into a computer-processable form on magnetic tape or disk. The computer system then processes the time records to develop a proof list showing the content of each record and containing arithmetic control totals that correspond to those developed by payroll. A control function in computer operations or in the payroll department compares the two sets of control numbers. Computer operations personnel are typically not authorized to proceed with the payroll process until all differences are resolved to the satisfaction of the payroll department manager.

This type of check and balance is used throughout a well-designed payroll system to ensure that the payroll department has full control over the operations done for them by the information services department. This design approach gives the payroll department the necessary authority to see that its responsibilities are carried out fully and accurately.

A second kind of interaction occurs when a new payroll processing system needs to be developed or the old one changed. The changes may be as minor as a new withholding schedule for social security or as major as a new labor contract requiring the development of entire new pay computing and reporting procedures. The process of changing existing computer systems, called system maintenance, is often as significant an activity for a business, in terms of resources consumed, as development of new systems. In either case, the payroll department works through the applications development group of the information systems department to create a new system or to change the existing system.

Other reasons for reprogramming the payroll system may be excessive complexity caused by frequent modification or the availability of more cost-effective equipment and methods. Many large computer systems are so complicated that no individual comprehends the whole; errors or bugs are continually found and corrected. Therefore, a computer program needs continual care and maintenance. Some programs are changed so significantly over long periods of time that their complexity increases, efficiency drops, and documentation becomes obsolete. In many instances documentation becomes so poor and the program so complex that the projected cost of continuing maintenance is greater than the cost of completely rewriting the system.

The payroll department retains full responsibility for the completeness and accuracy of the changes made to the system. Payroll must be satisfied that the system it receives from the information systems department satisfies the business requirements of the payroll department. Because payroll personnel cannot read and understand the computer programs that make up the computer system, they must rely on an audit of the results obtained from a real or theoretical trial or test of the system. These results are obtained in a process known as a "test run." In the test run, the computer performs the various processes in the new or revised system using a sample of information that will produce a known answer if the system is correctly programmed. A "parallel test" is often conducted in which a new system is run with the same input data as a proven existing system, manual or automated. The results of the two are then compared to ensure that the new system produces the same results.

User and information services departments working together on systems do not always achieve perfect results. Rather, the results reflect the organizational environment as well as the abilities and knowledge, or lack thereof, of the persons involved in the design and operation of the systems. Control steps are often overlooked or bypassed in the haste to make deadlines, or simply left out of the system design to save money.

To meet other deadlines, staff may put new or revised systems into production operation before testing is com-

pleted, sometimes with disastrous results. Seldom, if ever, do the users, designers, and programmers of systems foresee and provide for all possible eventualities. Seldom also do systems tests seek to verify all of the results obtained from all parts of the system acting both alone and together.

Computer systems suffer the shortcomings common to all complex systems. The computer, like other machines, faithfully performs as instructed when kept in good working order. However, the computer receives its processing instructions and raw material in the form of unprocessed data from people; it is therefore only one of the many parts of a payroll or any other system.

B. The Information Systems Organization

When computers were initially introduced into businesses and other organizations, they were normally brought in to address a single problem or business need. As a result, the information systems organization, or computer department, as it was probably called at the beginning, was usually a small unit of one or two individuals within the original using department. Because many of the first applications of computers in the business world were financial in nature—including general ledger, accounts payable/receivable, and payroll—the first information systems groups were generally part of the accounting or financial department. These first computer specialists did everything—designed systems, wrote programs, prepared input data, operated the computer equipment, and distributed reports.

As the use of the computer spread from its originating department to others, and finally throughout the business enterprise, the information systems organization likewise grew in size and scope. In many large businesses today, the information processing organization rivals the size of other service-providing departments. In addition, the manager of information services no longer reports to a single using department but to a higher authority, often to the president or other senior executive. The title of chief information officer (CIO) or the equivalent is practically as common today as chief financial or chief operating officer, especially in large companies that heavily depend on computers and information processing for successful business operation, such as banks and airlines.

Whereas the original computer departments contained a few individuals who were essentially jacks-of-all-trades, today's information systems organization consists of several subgroups, each having a number of employees performing the specialized functions of the group. A typical information systems organization within a large company includes the following major subgroups:

- Computer application systems development
- Computer operations
- Technical support.

Application systems development and computer operations are covered in detail later in this section. They are generally regarded as the areas with the greatest vulnerabilities for perpetrators of computer crime and therefore are of particular interest to investigators.

The technical support group is typically responsible for a variety of technical areas, including:

- Operating system installation, maintenance, and support
- Management and administration of the organization's data resources
- Short- and long-term planning for computer resources
- Analyst, programmer, and operations training
- Creation and maintenance of standards and documentation
- Support of end-users' ad hoc computing requirements.

In many organizations, end-user support has become sufficiently large and important to justify a separate support function. This group may be referred to as "end-user computing" or the "information center." Whatever it is called, its primary responsibility is to help users meet business requirements with application systems implemented on personal computers or workstations, or through the use of a very high-level programming language. These groups provide training, on-call programming assistance, and consulting to end-users interested in developing computer applications that would not fit normal production computer system guidelines. These ad hoc applications typically meet immediate, spur-of-the-moment needs and are used by only one or two individuals.

1. Computer Application Systems Development

Computer application systems combine specific human and computer methods, procedures, and processes that work together as a unified whole to produce a prescribed result. New systems begin with a functional specification that defines user functional requirements to be satisfied by the new system. A systems analyst who understands computer systems working with user personnel who understand the business needs typically develop the functional specification. After defining the users' information processing needs, the systems analyst determines the human and other resources, including the computer resources, required to meet those needs.

The resulting system design is documented so as to ensure effective and efficient execution of the system development phase and to assist with the subsequent installation, operation, and maintenance of the system. The systems analyst and one or more application programmers (see Appendix D) generally develop the system. (In many organizations, the same people perform analysis and programming functions, often called programmer/analysts.) The programmer codes the several computer programs that will become part of the final system, tests the programs against a set of sample information to ascertain whether they perform as required, and corrects them as necessary to ensure they produce correct results. The final stage of program testing includes installing all the programs on the computer and running them in a full production mode to determine whether they perform as planned. This step is known as the "systems test."

Few systems design and development projects follow these steps consecutively without some reversion to a previous stage. Systems design is often found faulty during programming, and programs often fail to mesh properly when the systems test is conducted. In these and similar situations, a part of the system is partially redesigned and/or reprogrammed. This process continues until satisfactory results are obtained.

The applications programmer works closely with the systems analyst during system development. The programmer codes and tests programs in accordance with the systems design, prepares test data, participates in the systems test, recommends system design changes to improve the system, prepares the completed program for installation in the computer operation, and documents the programs in accordance with accepted standards.

The programmer's task begins with a definition of the form and source of the data to be processed and the form and content of the results required. The programmer analyzes this information to determine the specific steps the computer will have to perform to produce the required results. The results of this analysis—the program design—are often recorded using graphical techniques (e.g., line-joined boxes and ovals) to show the overall program design and to serve as a road map during coding.

After the program design is developed, recorded, and reviewed for correctness, the required computer steps are entered into the computer in a form that is acceptable to the rules and conventions of the programming language used by the development organization. The set of program steps, coded in a programming language, is called a "source program."

Because newly coded programs are seldom if ever perfect, programs must be tested and debugged before they are used. The test consists of running many variations of data through the program, including some erroneous data, to ensure that the program does what it is designed to do and not what it is not supposed to do. The test run results are analyzed to determine whether they conform to the defined requirements of the program. If they do not, the programmer modifies the source program code and repeats the testing procedure until satisfactory results are achieved.

The final stage of program development is completing the documentation. Program documentation includes a collection of the information useful and necessary to the future use, understanding, and, where necessary, modification of the program. Complete program documentation usually includes:

- Narrative—a document describing the purpose of the program and the general solution used.
- Logic display—a description of the significant logical steps in the program, often in graphical form.
- Program listing—a printed copy of the source program (normally produced by computer).
- Input/output formats—a description of the data files, reports, and terminal screen layouts showing the relative location of each field in each record.
- Test data—a copy of the test data used to debug the program.
- Operator instructions—the instructions necessary to run the program on a computer. The format and content of these instructions are specified by the organization and vary widely.

The section of the computer services department responsible for designing and developing new computer application systems and for revising existing systems to meet new needs is usually called "systems and programming" or "application systems development." Most employees of such departments design systems, write computer programs, or both. In some cases, user departments perform development on a decentralized, less formal basis.

Computer systems design and development organizations vary with the size and complexity of their responsibilities. A small, limited computer installation may depend entirely on vendor-supplied and purchased systems; it will often have just one or two systems employees who devote their time to testing and installing those systems. The large, comprehensive computer installation may employ hundreds or even thousands of systems design and development personnel. Typical organization structures by size are summarized below.

Small Systems Departments—These departments typically consist of several persons, each reporting to the computer center manager and each performing all the tasks

necessary to design and develop systems; the computer center manager often does part of the systems design and development work.

Medium-Sized Departments—Medium-sized departments typically contain at least one manager or supervisor reporting to the computer center manager. This person is responsible for the programming work and perhaps the systems analysis and design also. Specialization between systems design and programming also begins at this stage. Systems programming, involving maintenance of the software controlling the computer, appears as a specialty, reporting either to the programming manager or the computer operations manager.

Large Departments—The specialization first encountered in the medium-sized department is extended further in the large department, usually to include manager and staff devoted to systems analysis and design, a separate manager and staff specializing in applications programming, and a third group specializing in systems programming. Additional specialists, including technical writers, training and educational personnel, librarians, and standards personnel, also appear in very large organizations. The several department managers may report to the computer center manager or to an intermediate manager of systems and programming.

Large systems projects usually require the participation of several specialties. Staff from the several departments are often assigned to work together on project teams to conduct this work, usually under a project leader who is typically the most experienced member of the team, often a senior systems analyst. The project team carries the project through to installation and successful operation of the system. The team is then disbanded, with its members returning to their respective specialty organizations and a program maintenance team takes over.

2. Computer Operations

A computer operations center can function in many different organizational configurations. Typically, however, its two major divisions are production support and equipment operations.

a. Production Support

The production support group often is concerned with several activities. Each is capsulized below.

Data Capture—The capture of data for input to a computer system consists of two steps. The first step is the physical gathering of data from such sources as orders, time reporting records, sales slips, recordings, or electronic sensors. After they have been gathered, the data must be converted into machine-readable form.

The second step, the conversion of source data, may occur at an operations center or at originating departments within the user organization. The data may take several forms: keyed directly to a computer using a computer terminal; keyed onto magnetic or optical media, such as tape, disk, or diskette; typed or printed onto sheets or cards to be read by an OCR (optical character recognition) or MICR (magnetic ink character recognition) reader; or punched into cards or paper tapes. The use of punched cards or paper tape has decreased significantly compared to other input forms, but they are still found in many large organizations.

To detect errors that may have occurred in the keying of data, a second operator may verify the data by rekeying the same data using the same medium as the first operator (i.e., computer terminal, magnetic or optical disk, magnetic tape, or punched cards). The purpose of verification is to determine differences, if any, in the way the two operators keyed the data. The differences are resolved and, if necessary, corrected data are prepared.

Manual checking methods are generally used to edit or verify the significant data or input that are typed on to sheets to be read by an OCR reader. In some cases, control totals of batches of data and sequence numbering of records are done manually and checked by the computer subsequent to input.

Scheduling and Coordination—As its name implies, this function establishes and maintains production schedules, monitors the production job stream, and makes adjustments as necessary. It also provides a point of contact for users, helps them enter jobs, and expedites work through the operations center.

Job Setup and Control—This function is often part of the scheduling and coordination function. It handles individual jobs as they enter, flow through, and leave the operations center. Controls are established and maintained; jobs are logged in; inputs are reviewed and edited as required (by the systems designer and user); jobs are made up by assembling job control cards, computer media, and files; and outputs are reviewed and prepared for distribution.

Library and Services—These services maintain the tape and disk library and other operations libraries and provide support services (such as supplies inventory) to the operations center. These functions are sometimes found in equipment operations rather than production support, particularly when jobs originate and are output at a remote teleprocessing terminal. In such a case, the library responds to instructions relayed to it by the operating system rather than the job set-up and control unit.

b. Equipment Operations

The equipment operations/computer processing group is concerned with several activities. Each is capsulized below.

Data Preparation—Preparation of computer input data usually consists of putting the machine-readable records in the proper sequence called for by the program and performing editing and validation functions to ensure that the input meets certain criteria, that values in certain fields are within prescribed limits, or that the codes in certain fields are consistent with the codes in other related fields. Many types of equipment can put data records in sequence or merge them with other records.

Computer Processing—After data have been edited, the next steps are computer processing and output of data. Processing and output generation are susceptible to two types of errors that computer operations staff must recognize and handle: program and equipment. The use of a formal development methodology including peer reviews and careful programming and testing can prevent many, if not most program errors. A computer itself can be programmed to identify some programming errors. For example, an instruction within a program that attempts to access main storage outside of the program's limits is an invalid command that most computers will detect. If such an error is detected, a computer will generally stop processing that particular program and go on to the next program. This event is called a program abort or an abend (abnormal end). Operations then notifies either the user or the responsible programmer to supply a remedy.

Computer circuitry malfunctions are rare because modern electronic circuits and components are extremely reliable. In fact, computers are now so reliable that an undetected failure resulting in erroneous output almost never occurs. Most all current computers have built-in error detection and correction circuitry to overcome internal faults that would have shut down earlier computers; many even keep a record or log of errors so that maintenance personnel can replace faulty parts. Several of today's fault-tolerant computers will take a failing component out of service, place a telephone call to a central vendor maintenance facility, electronically order a new component, and notify maintenance personnel that a fault has occurred. Regularly scheduled maintenance of the computer also keeps failures to a minimum.

Operator errors constitute a significant percentage of computer system errors and can occur during any phase of data processing. Precautions taken to ensure error-free input, effective and efficient programs, and reliable equipment can be nullified if the computer operator makes a wrong decision, mishandles materials or data, or is careless in operating the system. Valuable time can be lost, and an entire job or system of jobs may have to be rerun. The cost of a rerun may be the least costly alternative in some applications, however. For example, in billing customers, it is usually far more important that the bills be accurate than sent out at a certain time.

Accordingly, the system developers must provide comprehensive and complete system operating instructions so that both the computer and terminal operators can follow the operations schedule and ensure proper turnaround time and processing consistency for each job. These instructions, often referred to as a run book, must be precise and explicit to ensure that the operations staff process the job correctly. Although originally paper documents, as the name infers, run books are now often stored in the computer, available for display through the computer system console or other computer terminal. These system operating instructions vary according to the size and type of the installation; however, the following list is representative of a standard run book's contents:

- Job Schedule: Listed here are the run frequency, processing deadline, run time, retention periods for input/output (I/O) files, and scheduling priority of the jobs.
- Action Commands: Computer-generated instructions and commands are given that call for operator responses to make the system perform a specific action.
- Error Correction and Recovery: The operator follows these procedures to enter optional override messages designed to bypass halts or properly suspend processing because of abnormal job termination. System restart procedures are also included.
- Input/Output Dispositions: This section addresses the disposition of input and output data from the remote and central sites.
- System Backup Procedures: Remote and central site backup procedures provide an alternative processing method in the event of computer, program, or operator error. These procedures include, but are not limited to, reassignment of peripheral and terminal devices.

In a remote job entry (RJE) environment, those procedures should be augmented by local (remote) procedures for data collection, inquiry, batch transmission, and data reception scheduling. These procedures should specify the availability of data, scheduling priorities, frequency of transmission, and transmission times, as well as remote backup procedures.

In summary, the systems designer and the user are both responsible for determining the parameters within which computer operations may be allowed to continue processing after some condition occurs that halts processing. The specific actions that an operator is to take are generally incorporated in the run book (or a step-by-step procedure for the operator). Deficiencies in the run book, which must take into account all the probable conditions that may

occur during application processing, are often the weakest link in the chain. This problem occurs because of the initial urgency connected with getting the system operational or because of later changes to the application program that are not reflected in the run book. In either case, the result may be to halt the system and delay processing, or worse, to allow processing to produce faulty output. For all these reasons, comprehensive tests and procedural reviews are undertaken at the initiation of a new application, or change to an application, to determine whether controls and operator instructions are adequate.

Storing and Accessing Data—Computer data files can be classified in various ways. They can be classified according to the method of accessing the data contained in the file or the purpose the file serves. For batch applications, files can either be sequential-access or direct-access, whereas online applications are almost always direct-access. Additionally, a file may function as a master, transaction (input), or output file.

Sequential-access devices store and release data in sequence, one record after another, whereas direct-access devices store and release data from any part of the medium as directed by a computer program. Direct-access devices, therefore, can be accessed wherever directed in a random fashion, and can also be used for sequential processing.

Optical and magnetic-character readers, magnetic tape drives, and punched card readers are sequential-access devices; they handle only sequential data. A magnetic tape has data recorded or magnetized on one side, and the tape drive has a stationary read/write head that either reads data from or records data onto the tape as the tape passes over the head. In a typical computer operation center, a master tape file may be mounted on one tape drive, a transaction tape file on another tape drive, and an output tape file on a third tape drive. The central processing unit (CPU) would determine, from the program stored in computer memory for that application, what data to write onto the output file from the data contained on the master and transaction input files.

In a direct-access environment, magnetic or optical disks are the direct-access devices. A disk unit typically consists of one or more platters or disks mounted on a vertical shaft that spins the disk. Each platter has tracks (logical grooves) arranged concentrically like a phonograph record. The tracks are accessed by one or more read/write heads mounted on arms. These arms and attached heads are moved by a servo motor that is part of the disk control mechanism to position them over tracks on the disk. The heads read and write data on the tracks that they are positioned over. In general, magnetic and optical disks operate similarly, with the primary difference being the physical manner in which the data are recorded on the device. Magnetic disks use the presence or absence of a magnetic charge to represent data on ferrite particles deposited on the disk. The charge is applied by an electronic mechanism contained in the head. Optical disks use a laser in the disk head to access data stored on the disk.

Magnetic disks are the prevailing direct-access technology used today because of their complete read/write flexibility and lower cost compared to optical disks. Optical media, however, are gaining in popularity because of the comparatively large amount of data that can be stored. The main disadvantage of current optical technology is that the disks can only be read by a computer system. The disks are created and data recorded using an off-line process. A variation of this technology is the so-called WORM (Write Once, Read Many) optical disk, but this too is still basically a read-only device. In the near future, we can expect the development of optical disks with complete read/write flexibility similar to magnetic disks. When this occurs, optical disks may well begin to replace their magnetic counterparts for most application requirements.

The computer writes or reads data on disks in much the same way as it would on magnetic tape. As data are put onto a disk, a table of contents, or directory, is built to provide information about the file, including the physical location of files on the disk. With this arrangement, a computer can find individual files in the order required by the computer program without searching through the entire disk (as must be done in a sequential-access tape processing system).

Because of this characteristic, when investigators search for information in magnetic computer media that may have been erased, they may still be able to recover the data; a file is often erased by removing the file's entry in the directory and not by actually erasing the file itself. In this situation, the contents of the file can be recovered using available utility programs.

In general, direct-access devices are more expensive than sequential-access devices, but provide much greater speed, versatility, and capacity; therefore, the production data files of most computer centers now reside permanently on magnetic disks, whereas in the recent past most production files were kept on magnetic tape. Regardless of the choice of storage type, most computer operation centers periodically back up their files with copies on tape; where disk files are used, the disk file is usually copied on to tape to be safely stored as a backup.

Magnetic media store more data per unit of volume than paper files, but are more susceptible to damage. Tapes can be crimped or stretched, and disks can experience read/write head crashes onto the magnetic surface.

Safety storage measures that are appropriate for paper are often inappropriate for a magnetic medium. Paper burns at 451 °F; the glue that binds ferrite particles to tapes and

disks melts at temperatures as low as 125 °F. Consequently, a fire-retardant vault that protects paper may provide only limited protection for tapes and disks.

File Retention and Backup—In view of the vulnerability of data stored on a magnetic medium, adequate file retention and backup are crucial. More files are likely damaged by human error than by disaster or sabotage, however. Unintended "erasures" are a prime cause of data loss on tape files. Valid data tapes may be erased because some data centers may still use unlabeled tapes, for example. Fortunately, use of tapes without labels is a relatively unusual occurrence in today's modern data centers.

Labeled tapes do not prevent accidents, however. Most operating systems have an option that permits a retention date or period to be placed in the internal label. With some operating systems, even when a retention period is specified in the label, the operator can ignore the console warning message and write over a tape that should have been saved.

Updating the wrong edition of the file can also destroy data. For example, the operator can mount the wrong edition of the file and ignore any warning messages from the operating system. The user may then fail to notice the problem when reviewing the reports.

Updating problems can also occur when there is more than one transaction tape during an update period. One tape may be used more than once or not at all. Unless the user has externally generated control totals, such operational errors can be difficult to detect.

On-line systems present another problem because there may be no record of the input transactions and the associated data changes. If a disk file is accidentally destroyed, reconstruction may be impossible unless the input is copied onto a tape or another disk during the data capturing operation.

Program as well as equipment malfunctions can also destroy or alter files to the point where the data are unusable. Files can also be destroyed by human errors. Tape cartridges and disk units are delicate. If someone grasps an unprotected tape reel by the outer edge rather than at the hub, the tape can be crimped such that it is unreadable. Similarly, dropping a disk pack can render the data it contains unusable. The design of most newer disk units, however, prevents this problem as the disk pack is no longer removable from the drive as was the case with older models.

Whereas operational problems usually destroy a single file or a limited number of files, disasters can destroy an entire library. Water and fire are probably the most common natural disasters facing a data center. In a sense, a computer center creates its own fire hazards—high voltages and highly combustible paper dust. Water from broken pipes, floods, and sprinklers used to extinguish fires likewise does great damage, although mostly to media since computer equipment can usually be dried out and restored.

Storage Location for Backup—All data centers have files stored in the computer room and/or an adjacent tape library. These on-site files may be inside a fire-retardant tape vault or safe, but more frequently they are on open shelves in a room that may be protected by automatic sprinkler systems. When a safe or vault is used, the operations manager may not use off-site storage, believing that the vault provides adequate protection. As previously discussed, this assumption may not be valid; off-site storage can definitely enhance file security. Because off-site storage is intended to provide protection against disaster, off-site facilities should be far enough from the on-site facility so that one disaster does not destroy both locations.

Testing the Usability of Backup Materials—Although department standards may stipulate updating procedures for backup programs, the procedures may not be properly followed. Moreover, although the standards may indicate which master and transaction files are to be stored off-site, the schedule may not be kept. The standards, therefore, normally include a procedure for testing the backup. For example, backup programs and files are usually used or tested at least annually; problems and failures are noted, and the standards are modified as necessary. An investigator searching for computer-stored evidence may often be able to find it at a backup facility if not in the main data center.

c. Typical Computer Operations Reports

Computer operations managers and others require reports on many operational functions. Usually produced automatically by the computer system, these reports often provide extremely valuable information to an investigator because of the detail they contain on the ongoing day-to-day, hour-by-hour operation of the computer system, its users, and application systems. The report names presented below are meant to be descriptive and may vary in actual data center usage.

Computer Operator Console Log—Chronological listing of computer system events and operator actions. The console log information is usually printed on continuous, page-numbered forms; it is also accumulated on magnetic tape or disk. The log identifies tape cartridges and disk volumes mounted, system or application programs used, assignment of job numbers to particular users, commencement and termination of specific jobs, and use of system resources, such as a line printer. It also directs impromptu operator actions. The log is the most comprehensive listing of computer system events. (Frequency: continuous)

Machine Room Access Log—Chronological description of all persons gaining access to the machine room. If visitors are admitted, their escort is also identified. Identification card/badge readers are often used to record this information in a microcomputer. (Frequency: continuous)

Processing Schedule—Explicit processing schedule showing the day and time at which specific jobs should be run. The schedule lists files to be used for the identified jobs where files are specified by tape number and date created. Applications and systems programs to be executed are delineated by program identifiers and accounts to be charged. Files may or may not be stored on magnetic tape cartridges. (Frequency: daily)

Daily Detail List—In-depth report of users accessing the system, the log-on and log-off times of these users, their priority codes, and accounting data relating to computer system resources consumed. Accounting data include computer processing time, I/O activity, and elapsed time connected to the system (connect time). Errors and warnings concerning accounting data, such as an invalid job order number, appear here. (Frequency: daily)

Computer Utilization Summary—Extracts data from Daily Detail List to perform statistical analyses. The summary provides a breakdown of the ways in which the computer was used (e.g., hours on-line, amount of time the processor was idle, I/O activity). Data may be presented by user, job order, application program, project, or division. This report is helpful in detecting unauthorized use of system resources. (Frequency: daily, weekly, monthly, year to date, on request)

Computer Utilization Accounting Control Report—Relates statistical data set forth in Computer Utilization Summary to accounting charges made during this period. This report shows total dollar accounting units for computer processing time, I/O activity, and the like. (Frequency: weekly)

Valid Job Order List—Describes job orders that are currently recognized and to which jobs may be charged. Jobs may originate within the organization or through a telecommunications network; accounts to which either may be charged are listed here. (Frequency: weekly)

Accounting Code Error Listing—Sets forth time, user, and other circumstantial details of errors in job order codes, user IDs, and the like. The listing helps in the detection of browsing and searches for accounts to which unauthorized activities may be charged. (Frequency: weekly, monthly)

Computer Utilization Summary by Priority Code—Description of ranks assigned to tasks that determine the precedence in which jobs receive system resources. The data are broken down by projects, divisions, locations, or users. The report shows disproportionate uses of system resources. (Frequency: monthly, year to date)

Terminal Usage Report—Details usage, as measured by connect time, for specific terminals. The report may contain the times at which a terminal was in use. (Frequency: monthly, year to date)

Computer Storage Summary—Provides a measure of on-line storage used by specific job orders and may also contain information on off-line tape reels and disk packs associated with a job order. (Frequency: semiannually, on request)

d. Computer Products and Supplies

Many companies supply computing equipment and related supplies and services. These companies distribute their products and services throughout the nation, usually through a network of sales and service offices and/or agents.

Typically, the larger computer manufacturers offer a wide range of products and services covering nearly everything a computer user might need. Many smaller companies selectively compete in just one or a few of these product areas. Nearly all computer installations use multiple vendors.

Equipment manufacturers affix to each machine a permanent tag showing the manufacturer's name, the unit serial number, and other information such as time or place of production. The information from this tag is sufficient to identify the supplier in most cases, thereby enabling the user to contact the equipment manufacturer to answer any inquiry regarding the functioning of the equipment.

Other items, such as programs, supplies, and services, cannot be so readily tracked to their source. Inquiries must usually be addressed to the data processing professionals in the organization who are familiar with their department's use of all such supplier-provided items.

C. Physical Facilities for Computers

The way a large data center protects its assets depends on top management's perception of the data center's importance to its business and thus its willingness to invest the necessary resources to secure those assets. For example, a bank obviously has a greater need for control than a mail order house with small dollar value sales. Similarly, the extent to which a business may or may not adopt different types of control, security measures, mechanisms, and procedures depends on its size, its economic strength, the sensitivity of its data, and the regulations imposed by government or other auditing agencies.

Because of the great number of differences among data centers, this manual cannot cover all of them. Therefore,

the following sections describe a large, idealized data center that needs comprehensive operating control and security. Scaled-down versions can be applied for data centers whose needs are less critical. Computer centers do not necessarily have all of the features described here, however.

1. Protection Facilities

Fire protection and detection, annunciation panels, mantraps, guard stations, access control devices, telephone, and internal communication procedures and devices are common elements in the effective operation of a large corporate data center.

Fire Protection and Detection—Fire protection and detection have several components: the number, kind, and location of fire alarms; fire extinguishing equipment such as water sprinklers and Halon gas; fire department notification methods; the use of nonflammable and nontoxic materials; and the cables and wiring that are used in the data center.

Annunciation Panels—Annunciation panels are used to signal abnormal conditions, including fluctuations in electrical power, water detection, fuel levels in power generators, status of coolant pumps, and unauthorized entry and intrusion alarms.

Mantraps—Mantraps are usually sequential entry double doors or turnstiles at computer room entrances activated by security guards inside the guard station or by keycard. Frequently, they include keycard door locks, audible alarms, closed-circuit TV surveillance, and metal detectors. A mantrap generally assists the security guards to detain a person attempting to enter or leave the computer room until the guards are satisfied that the person is authorized to be there and presents no threat to the center.

Guard Stations—A guard station is a specially constructed and designed enclosure that is usually connected to, or part of, the mantrap. Often, these stations are manned 24 hours per day, 7 days per week. They are equipped to monitor the security of the data center through TV monitors, public address speakers, direct manual alarms to police, private security service, and fire departments, intercoms with the data center, TV surveillance and automatic photographing of persons entering the facility, radio police scanners tuned to emergency channels, walkie-talkies for emergency communications, and sometimes a wide array of automatic shutoff switches to reduce harm to the equipment in the event of detection of some abnormal function occurring within the center. They are often constructed with bullet-proof walls, doors, and windows, depending on the nature of the perceived threat to the data center and required protection capabilities.

Access Controls—Access controls often include card-key locks, automatic door closing, fingerprint or photo identification and other means of logging in, and cameras trained on entrances, hallways, loading docks, elevator doors, outside building entries, and potentially vulnerable public access areas above, below, and around the data center. These controls also might include mirrors to eliminate blind spots in these same areas and emergency lighting units to be turned on in the event of failure in the regular lighting system.

Internal Communications—Internal communications include intercom systems among guard stations and all areas concerned with the daily operation of the data center. Generally, the systems provide the guards with override capability of all stations, conference calling capability, and busy line indicators. As mentioned above, direct communications lines with police and fire department are often provided, as well as walkie-talkies and public address systems to all data center areas.

Telephone Service—The telephone system installed must be reasonably secure against willful or accidental damage. Consequently, the wiring of the system is often under the raised floor, encased in fire-protective materials, and equipped with smoke and heat detectors. Generally, several lines are used in case one becomes inoperable. The telephone wire terminal closets are locked and within the secure perimeter.

2. Technical Computer Safeguards

Numerous computer safeguards are available; several books listing them have been published[1, 21]. An investigator or prosecutor will encounter many of them in any case of suspected crime, and should ask the victim to have all safeguards that were or could have been involved described and documented. Technical safeguards in computer systems include data file protection, storage partitioning, protected or privileged mode for operating system programs, encryption, exception reporting, and access control, to name but a few.

An example of a comprehensive computer safeguard shows the complexities involved. The safeguard is password access control in an on-line, multiaccess computer system. A user accesses the computer through terminals; that access is controlled by having the identity of the terminal user authenticated with a secret password known only to the user. An effective password capability normally has the following characteristics:

- Passwords are sufficiently long to reduce the possibility of guessing.
- The user selects passwords after initial access to the system; thereafter, the system forces changes in passwords on a periodic basis, typically 60 days.

- A password being entered at a terminal is not visible on the screen or to other people in the area, nor is it visible on any printed paper coming from the terminal.
- Password holders are periodically indoctrinated about the secrecy of their passwords and their responsibility for safeguarding passwords.
- Safe password administration is required, including elimination of or imposition of strict security on password lists, frequent password changes, separation of duties in the administration of passwords, accountability for the safety of passwords, and background investigation of those people in high positions of trust who administer passwords.
- Password lists stored in the computer and used for authorization purposes are encrypted. As soon as a password enters the computer from a terminal, it is immediately encrypted and compared against the master password in encrypted form only. This feature reduces the exposure of actual passwords in the computer.
- Time delays are imposed on terminal users so that repeatedly attempting to use unauthorized passwords requires discouragingly large amounts of time. Also, an individual is not allowed to input an incorrect password more than three times before being disconnected.
- The system displays a banner message during the logon process warning users and potential intruders about trespassing.
- All system logon attempts, successful or not, are recorded, or logged, by the computer system. The computer then analyzes the data files produced and produces exception reports indicating deviations from normal use that might indicate attacks on the system.
- Procedures are established for imposing alternative methods of security when the password system and the computer equipment supporting it fail to function properly.
- Sanctions are clearly known by password holders, and violators are punished.

If a password system does not include at least these characteristics, it is probably not an adequate safeguard for the resources it is meant to control.

3. Operation and Production Areas

The principal component of the operation and production areas to be considered in data center design are the computer room, operation center, libraries and vaults, and the vendor service engineer area. These are described below.

Computer Room—Because the computer room is the heart of the data center, it must be designed for effective, reliable, and low-risk operation. It must therefore be located away from rooms containing major mechanical and electrical equipment and away from places that are subject to flooding or water main breaks. A secure computer room usually has a solid ceiling as well as steel and concrete walls and doors that are fire-resistant for at least 2 hours. Usually, the computer room has no windows or skylights; if it has, these are permanently sealed and fit with appropriate alarms.

The most common type of floor is the raised or free access type. Raised floors serve several practical purposes. Cables placed under the raised floor do not obstruct aisles. Air-conditioning conduits to computer components may be ducted under the raised floor, or the entire space may serve as a plenum with conditioned air under pressure directed to vents near the components. Each panel of the floor, usually 24 inches square, is removable for access to the space below. The distance between the subfloor and the raised floor generally ranges between 15 and 24 inches. The floor panels are guaranteed against static buildup and easily cleaned.

The layout of the computer room is designed to ensure efficient work flow, to permit sufficient aisle clearance for hand trucks or equipment, and to provide sufficient space for equipment maintenance. Traction pads are installed on all ramps to prevent slippage. Printers and card devices are located for the most convenient access to supplies; however, such peripheral equipment is usually located away from disk and tape drives and other electronic devices (such as the processor and memory) because of the paper dust these devices generate. Fire extinguishers are both strategically located for easy access and frequently inspected. Signs indicate the type of fire extinguishers that can be used and how to use them. Similarly, other signs are placed in critical areas to instruct personnel on the use of other safety devices such as power cutoff switches and evacuation routes.

Operation Centers—The operation center is a room generally used for production control, scheduling, and user coordination. Although it often is located inside a computer room, the operation center should be situated elsewhere because traffic and security problems should be minimized in this area. It may also be adjacent to the guard station so as to provide the surveillance, protection, and communications that are available from these stations.

Libraries and Vaults—Libraries and vaults generally are located in a room just off the computer room, but only one entrance is provided directly from this room into the computer room. The same steel and concrete construction is

used here as in the computer room, and similar alarm devices and surveillance methods prevail. The humidity and temperature controls, however, are separate or independent from the computer room and have a backup capability in case of failure of the main system. The floor supports in this room generally require greater strength because of the weight of safes and other heavy containers. Safes are usually rated to ensure their proper use; that is, as indicated earlier, some safes adequately protect paper documents such as check stock but are not sufficient to protect magnetic tape media. Sometimes, safes have automatic door closing in case of a fire or other emergency.

Vendor Service Engineer Area—The vendor service engineer area is located away from the computer room and general traffic flow, but it usually is within easy access of the computer room. The computer and peripheral equipment vendors' engineers who maintain the computer system have offices next to the documentation, spare parts, and test devices necessary for monitoring the system. Leakproof, lockable, fire-proof cabinets are used to store a minimal supply of cleaning solvents necessary to maintain equipment.

4. Mechanical and Electrical Support Facilities

Several mechanical and electrical support facilities are found in the data center. These are briefly discussed below.

Electrical Power—A data center is totally dependent on electrical power. The organization thus provides separate rooms, often on a lower floor, to store equipment necessary for daily processing operations and for emergency backup. Some of the types of equipment that are stored in those rooms include: uninterruptable power supplies (UPS) such as batteries, diesel generators and control circuitry; fuel tanks for diesel generators; motor generators for CPUs; water chillers; spare fuses and fuse panels; and other spare parts and tools. The rooms are equipped with floor drainage with backwater valves, smoke and heat detection, water sprinkler systems or Halon gas fire suppression systems, carbon dioxide and water fire extinguishers properly placed, humidity and temperature indicators and controls, bypass switches for emergencies and maintenance, devices to record variations in input power, transformers specifically for the data center, watertight outlets beneath the floor, and all the surveillance and communications previously mentioned. Most important, the data center electrical system is separate from other building facilities, and equipment is available to back up this system when required. These rooms have an inconspicuous location requiring infrequent access by facilities engineers.

Lighting—Artificial lighting is provided throughout the data center because of the scarcity of windows. Aside from the requirements of candle power, which will vary by area, emergency lighting (battery-powered lights) is available throughout the data center, in the mechanical and electrical equipment rooms, and in critical surveillance areas. These systems are connected to the annunciation panels and can be controlled from inside the guard station.

Air Conditioning—Although the need for air conditioning in data centers is obvious, the normal ventilation system frequently cannot produce a reasonably trouble-free environment. Too often the air conditioning that supplies the building is also used to supply the data center. Air conditioning for a data center should be separate and provide for a backup capability. Additionally, special air intake devices are sometimes used to protect against noxious fumes or corrosive materials entering the environment. Air filters conform to UL Class 1 and are easily accessible for inspection and replacement. Several portable temperature and humidity records are located throughout the data center. Critical spare parts are stored on site.

Motor Generators—Some CPUs require motor generators or electronic regulators to provide a level and quality of power different from standard commercial power. Spare units are on hand to back up primary units; these are equipped to automatically cut over in the event of a primary failure. Located to provide easy access for on-site repair, maintenance, and manual testing, they need to have sufficient capacity to be able to take a unit off-line without service interruption. They also are connected to annunciation panels and other signal devices to warn of potential damage.

Water Chillers—Like motor generators, some CPUs require water chilling equipment to provide a constant appropriate temperature. The same backup protection that applies to motor generators applies to water chillers.

Uninterruptable Power Supply—A UPS system provides electrical power to the data center in case of a commercial power failure; it also allows a return to commercial power or other separate power sources. Because it provides power for computer equipment, lighting, telecommunications, motor generators, annunciation panels, security controls, security equipment, and other means of automatic entry and exit such as doors and elevators, the UPS system requires weekly testing of the entire system. The UPS system also protects against unexpected surges in power that might otherwise damage the data processing equipment in the system.

5. Other Areas Related to the Data Center

Several other areas are related to the data center. Any reception room for visitors and users is located outside the data center. Pickup stations for delivery or pickup of materials are adjacent to other data center areas. Elevator shafts are not common to any walls of the computer room, other data center rooms, or critical areas. If an elevator is

necessary, its use is restricted to data center personnel or authorized personnel; moreover, it is connected to a monitoring system in the guard station when the elevator stops at the data center level. Operators' lounges are frequently provided, particularly in installations that have 24-hour operations. Preferably they are not accessible except through the data center.

Janitorial rooms have central access to the data center so that adequate cleaning and maintenance may be efficiently performed. Because various cleaning supplies are stored and these rooms are generally equipped with deep sinks, these rooms should be protected against fire and water damage as well as the extension of that damage to the data center. Accordingly, those rooms are constructed in much the same way as the computer room (except for the raised floors) and have the same kinds of protective devices to monitor against potential damage.

Locker rooms and rest rooms are not located adjacent to the computer room or any critical mechanical and electrical equipment rooms or facilities. Nevertheless, because these rooms obviously must be reasonably close to the data center, they should have a public address system and protective devices against fire and water damage. For the same reasons, these rooms have no windows or other means of access that would present vulnerability to the data center.

Storage and supply rooms are used to provide materials for efficient operation. These rooms are not located next to the computer room or mechanical and electrical equipment rooms because the materials they contain often are combustible. For this reason, these rooms have intercom stations, fire extinguishers, water systems that are independent of all other data center areas, floor drains with backwater valves, water alarm connections to annunciation panels, and intrusion alarm systems that are monitored by the guard station.

D. The Impact of Data Communications

The rapidly expanding use of data communications technology has affected all of the areas discussed so far in this section and will continue to have a significant impact on computers and data processing in the future. The specific impact on these areas is described below.

Aside from understanding the basic nature of the technology and its impact on the industry, computer crime investigators should realize that data communications has essentially eliminated the geographic constraints on computer crime. No longer need perpetrators be physically near the computer system and its data; they can be in another part of the country, or even in another part of the world.

1. Computer Usage

Computer users from the scientific and engineering disciplines have routinely used data communications for many years. Time-sharing systems have long been common in this environment and continue to be heavily used for research and other such technical activities. The primary change in today's laboratory is the widespread use of intelligent workstations connected to a network of server devices rather than the simple, dumb terminals connected to a large computer that were originally used for time-sharing applications. These workstations have computing power, file storage capacity, and graphics output capabilities that are, in many cases, greater than the previous generation of large mainframe computers. The scientist or engineer develops application programs on the workstation and executes many of the programs there as well. The workstation is typically connected to a data communications network that provides access to other specialized computing capabilities not available on the workstation, such as vector processors for intense computation, data base machines for complex data access requirements, and network gateways for access to remote computer systems and users.

Through the workstation and the network, scientific and engineering users have access to whatever computing capabilities are required to complete their job. These users have taken advantage of new computer and communications technology, but the basic problem-solving nature of their computing work has not changed substantially.

On the other hand, continuing implementation of data communications technology over the last 10 to 15 years has slowly but dramatically changed the manner in which computers are used in businesses and other organizations. Although this period may seem to be a long time, the change from the original paper-based batch computer systems to today's trend toward on-line transaction systems has required the business community to make a heavy investment in both computer and people resources. Scrapping functioning batch computer systems and redeveloping on-line systems to replace them can be a difficult decision for management, particularly in times of tight financial constraints. In recent years, the need for a business to remain competitive or to gain a significant competitive advantage through the use of on-line transaction systems has been a strong motivating factor in many redevelopment efforts.

In the early 1970s, only a few businesses used large transaction processing systems that took full advantage of data communication capabilities. Airline reservation systems, teller networks for large, multibranch banks, and innovative use by a few large retailers constituted the major on-line systems in use at that time. A number of smaller systems existed, but these were generally limited to a few

terminals located relatively close to the computer center serving a single application. In the mid-1980s, practically all computer applications have some on-line component, with many having nationwide networks and thousands of terminals. The most visible of these include bank automated teller machine (ATM) networks, credit card authorization terminals, and the variety of point-of-sale (POS) systems being deployed by all types of retail establishments.

This change in the nature of computer applications has affected the controls used in applications. The first computer systems had a single input device, usually a card reader, and a single output device, usually a printer, both located in the computer room and operated by trained and trusted staff. The mechanisms and procedures necessary to control and secure this environment were far simpler than today, where an on-line system may have thousands of widely dispersed input/output devices (terminals) in the control of operators that may not be equally well qualified.

As data communication systems have proliferated, computer application systems have become more sophisticated and complex. In response, the security and control measures necessary to protect the systems and guarantee data integrity and availability have also become more complex—as well as more critical to successful operation of the business.

2. The Information Systems Organization

The primary change in information systems groups resulting from increased use of data communications has been the addition of specialists to work with the new technology, particularly in technical support and computer operations. Data communications technology has not affected the application systems development process as substantially; additional training of existing staff has generally been sufficient.

In the technical support area, technicians with communications network design and planning skills are required to help design the large networks that many businesses are establishing. A nationwide (in some cases, worldwide) network can be a very expensive resource for an organization to install and maintain. Often, several options are available for routing lines to the various nodes on the network, each with varying costs and service capabilities. Backup service must also be considered.

In addition to network planning, technical support staff must install and maintain new system software. On-line systems require teleprocessing monitors or similar software both to control the flow of input transactions and resulting output messages, and to schedule the work of the computer system. In many cases, on-line computer applications use a data base management system (DBMS) for controlling and accessing the data required by the application.

Operation of a large on-line data communications network may be more difficult and complex than operation of the computer system(s) for which it provides service. In most organizations, the computer operations group also performs network operations, although separate network groups are not uncommon. Network operation requires staff with special skills and training in data communications as well as knowledge of the operation of the computer system.

Unfortunately, networks tend to be dynamic, somewhat unstable, typically requiring constant attention to ensure efficient operation. The network control staff must continually monitor the status of communications lines, line concentrators, terminals, terminal control units, and other equipment. When a problem in the network occurs, they must diagnose the problem quickly and perform whatever actions are necessary to correct it. These actions may be as simple as substituting a piece of equipment in the network configuration to replace failed equipment. At the other extreme, solution of the problem may require contacting the telephone company or other communications provider (there may be more than one) and replacing one or more of the communications lines in the network and associated equipment.

As a normal part of their job, network operations staff have access to and use a variety of monitoring and test equipment that introduce security vulnerabilities into a data center. The use of this equipment must be carefully monitored and controlled to ensure that it is not used for unauthorized purposes.

As an example, a commonly used tool is a data scope—a monitoring device that attaches to a communications line and displays all the data that are passing over the line in real time. Many data scopes also can record the data on tape cassettes for later playback. A perpetrator with access to a data scope could attach it to a line for an extended period of time, recording all data going in and out of the system on that line, including user IDs and passwords for users accessing the system from terminals on the line. Since these data are usually in clear text—not encrypted—and readily identifiable, the individual could later access the system by impersonating a legitimate user.

3. Physical Facilities

Organizations with a data communications network typically have a separate network control center for operating the network. This center is located in or adjacent to the computer operations center because of the requirement for almost constant communication and coordination between the two facilities.

For a small network, network control may be little more than a desk near the modem rack with space for monitoring and test equipment. The control center for a very large

network may resemble a space-age military operational command center, with a large, lighted, electronic map showing the status of network components, panels of flashing display lights, complex switching and routing equipment, on-line diagnostic equipment, and multiple VDTs for simultaneous monitoring of network-related displays.

The environmental, access control and security, and other physical requirements for a network operations center are the same as already given for computer operations.

4. Future Considerations

As stated above, data communications systems are important to investigators and prosecutors because they have essentially eliminated the geographic constraints on computer crime. A criminal action can be initiated from practically any location with the right resources, even from a laptop computer in a telephone booth.

Another technological advancement that many organizations are planning or implementing and that will affect the investigation and successful prosecution of computer crime is distribution of computing capabilities. Distribution of computing away from a central facility is facilitated by data communications technology.

Distributed processing implies moving the computer processing power as close to the end-user as practical. The use of personal computers in the office and elsewhere is perhaps the simplest and most striking example of distributed processing. At the next higher level, departmental or office systems provide processing capabilities for groups of people with common requirements, such as document storage and retrieval for a legal department. The mainframe processing capabilities of the data center are used for applications that are used by all or most employees or that require access to data that are used by the entire organization.

In this hierarchical arrangement, each level is connected to the next higher level via a communications network. Data are distributed vertically—that is, the data reside at the lowest level possible in the hierarchy to meet user needs. A transaction entered through a personal computer that requires access to data at a higher level is passed to that level for execution. In a vertically distributed environment, a transaction will eventually find the data required for execution at the highest level, typically the mainframe computer(s) of the corporate data center.

Horizontal distribution of data changes and complicates this scenario considerably. Horizontal distribution implies that an organization may have more than one, perhaps many, highest levels. For example, a business with several divisions may have a data center in each division, independent of the others. Within each division, processing and data are distributed vertically. A transaction requiring data concerning more than one division would need to access data stored at each of the respective division data centers to complete successfully. This transaction can be completed with current technology if the transaction is very well defined and the several computer systems and data bases involved are homogeneous.

At the other extreme are ad hoc queries to heterogeneous data bases and systems, i.e., nonspecific, unstructured requests that may involve access to differently organized data on several kinds of computer systems. Completing such a transaction is all but impossible with currently available technology. This type of capability is needed, however, and research is slowly progressing toward satisfying the requirement.

These and other future technology changes resulting from the increasing use of data communications technology will continue to complicate investigation and prosecution of computer crime cases. Fortunately, many of the tools necessary to implement, monitor, control, and understand the operation of these complex data processing environments will also be of value in the discovery and investigation of computer crime.

E. Computer System Vulnerabilities

Many computer system vulnerabilities seem obvious, but some of them—even the important ones—can be overlooked. To assist the investigator, two analyses of the principal vulnerability found or surmised in recorded cases of computer abuse are presented below[28]. The first analysis is based on a breakdown of common functional weaknesses, such as inadequate I/O controls; the second is based on a breakdown of the most common functional and physical locations of vulnerabilities.

1. Functional Vulnerabilities

The following functional vulnerabilities emerged from the analysis:

- Manual handling of input/output data
- Physical access to EDP facilities
- Operations procedures
- Business practices
- Computer program usage in micro- and mainframe computers
- Operating systems access and integrity
- Teleprocessing service usage
- Magnetic tape and diskette handling.

Each vulnerability is summarized below in order of frequency of occurrence. Examples that demonstrate the range of acts facilitated by each vulnerability appear in Appendix C.

Poor Controls over Manual Handling of I/O Data—The greatest vulnerability occurs wherever assets are most exposed. During the past 30 years—the period of reported cases—assets have been most tangible and subject to human acts before entry into computers and after output from computers, typically where perpetrators rely on failure to detect false data entry into the computer. Data assets are more accessible outside computers than when they are within them and programs must be executed to achieve unauthorized access. Controls that are often absent or weak include separation of data handling and conversion tasks, dual control of tasks, document counts, batch total checking, audit trails, protective storage, access restrictions, and labeling.

Weak or Nonexistent Physical Access Controls—Where physical access is the primary vulnerability, nonemployees have gained access to computer facilities, and employees have gained access at unauthorized times and in areas in which they were unauthorized. Perpetrators' motivations have included political, competitive, and financial gain. Financial gain occurs mostly through unauthorized selling of computer services, holding computer centers for extortion purposes, burglary, and larceny. In a number of cases, the motivating factor has been employee disgruntlement, sometimes stemming from frustration with various aspects of an automated society. Inadequate or nonexistent controls involved door access, intrusion alarms, low-visibility of assets, identification and establishment of secure perimeters, badge systems, guard and automated monitoring functions (closed-circuit television), inspection of transported equipment and supplies, and staff sensitivity to intrusion. A number of intrusions occurred during nonworking hours when safeguards and staff who might notice intrusions were not present.

Computer and Terminal Operational Procedures—Losses from weaknesses in operational procedures have resulted from sabotage, espionage, sales of services and data extracted from computer systems, unauthorized use of facilities for personal advantage, and direct financial gain associated with negotiable instruments in operational EDP areas. The controls whose weakness or absence facilitates these kinds of acts include separation of operational staff tasks, dual control over sensitive functions, staff accountability, accounting of resources and services, threat monitoring, close supervision of operating staff, sensitivity briefings of staff, documentation of operational procedures, backup capabilities and resources, and recovery and contingency plans. The most common abuse problem has been the unauthorized use or sale of services and data. The next most common problem is sabotage perpetrated by disgruntled EDP operations staff.

Weaknesses in Business Ethics—A weakness or breakdown in business ethics can result in computer abuse perpetrated in the name of a business or government organization. The principal act is related more to a company's practices or management decisions than to identifiable unauthorized acts of individuals using computers. These practices and decisions result in deception, intimidation, unauthorized use of services or products, financial fraud, espionage, and sabotage in competitive situations. Controls include review of business practices by the company board of directors or other top level management, CPA audits, and effective practices of regulatory and law enforcement agencies.

Weaknesses in the Control of Computer Programs—Programs are assets subject to abuse; they can also be used as tools in perpetrating abuse. The abuses from unauthorized changes are the most common. Controls found lacking include labeling programs to identify ownership, formal development methods (including testing and quality assurance), separation of programming responsibilities in large program developments, dual control over sensitive parts of programs, accountability of programmers for the programs they produce, the safe storage of programs and documentation, audit comparisons of operational programs with master copies, formal update and maintenance procedures, and establishment of ethical concepts of program ownership.

Operating System Access and Integrity Weaknesses—All of these recorded compromises of computer operating systems involve the use of time-sharing services. Compromises are accomplished through discoveries of weaknesses in design or taking advantage of bugs or shortcuts that programmers introduced while implementing operating systems. The acts involve intentional searches for weaknesses in operating systems, or the unauthorized exploitation of weaknesses discovered accidentally. Students committing vandalism, malicious mischief, or attempting to obtain computer time without charge have perpetrated most of the acts in university-run, time-sharing services. Controls to eliminate weaknesses in operating systems include methods for proving the integrity and security of the design of operating systems, imposing sufficient implementation methods and discipline, proving the integrity of implemented systems relative to complete and consistent specifications, and adopting rigorous maintenance procedures.

Poor Controls over Access to Teleprocessing Services through Impersonation—Unauthorized users can most easily gain access through impersonation by obtaining secret passwords of legitimate users. Perpetrators learn passwords that are exposed accidentally through

carelessness or administrative failures or obtain them by deceiving people into revealing their passwords or by guessing obvious combinations of characters and digits. The latter technique has been facilitated by programmed microcomputers that can repeatedly try thousands of combinations in short periods of time. This type of abuse may be so common that few victims bother to report cases. Control failures include poor administration of passwords, failure to change passwords periodically, failure of users to protect their passwords, poor choices of passwords, absence of threat monitoring or password-use analysis in time-sharing systems, and failure to suppress or obliterate the printing of passwords.

Weaknesses in Magnetic Tape and Diskette Control—Theft of magnetic tapes and diskette, their destruction, and data erasure from them are acts attributed to weaknesses in control of magnetic tapes. Many other cases, identified as operational procedure problems, involved the manipulation of data on tapes and diskette and copying. (No cases are known in which magnetic disk packs have been subject to abusive acts.) Controls found lacking include limited access to tape libraries, safe storage of magnetic tapes, the labeling of tape reels, location and reel number accounting, control of degaussing equipment, and backup capabilities.

2. Functional Locations of Vulnerabilities

The primary functional locations of vulnerabilities that emerged from the analysis were:

- Data and report preparation
- Computer operations
- Information workers' offices
- Computer systems usage
- Programming
- Magnetic tape storage.

These are summarized below in order of frequency of occurrence. Use of a computer terminal in a computer abuse act is considered separately from acts committed without a terminal for the areas where terminal usage is relevant and can be separated.

Computer Data and Report Preparation Facilities—Areas included key-to-tape/disk/card data conversion, computer job setup, output control and distribution, data collection, and data transportation. Input and output areas associated with on-line remote terminals are excluded here.

Computer Operations—All functional locations concerned with operating computers in the immediate area or rooms housing central computer systems are included in this category. Detached areas containing peripheral equipment cables connected to computers and computer hardware maintenance areas or offices are also included. On-line remote terminals (connected by telephone circuits to computers) are excluded here.

Information Workers' Offices—Many cases in this category involved business decisions in which the primary abusive act occurred in non-EDP areas such as management, marketing, sales, and business offices.

On-Line Terminal System Usage—The vulnerable functional areas are within on-line computer operating systems where acts occur through execution of programmed instructions.

Programming Offices—This site includes office areas where programmers produce and store program listings and documentation.

Data Preparation and Output Report Handling Areas with On-Line Terminals—This category includes the same functions identified in the first discussion of data preparation facilities, but is associated here with on-line terminals rather than computers.

Magnetic Tape Storage Facilities—Areas include tape libraries and any storage place for tapes containing usable data, but exclude temporary or short-term storage of tapes in tape drive mounting areas. The latter is included in categories discussed above on computer operations and computer data preparation facilities.

On-Line Terminal Operations Areas—This category is the equivalent of the computer operations discussed above, but is in on-line terminal areas.

Central Processors—These functional areas are within computer systems where acts occur in the computer operating system but were not induced from terminals.

3. Accidental and Intentional Losses

Errors and omissions occur most frequently in labor-intensive functions where detailed, meticulous, and intense activity requires concentration. The vulnerabilities are usually manifested in data errors, computer program errors or bugs, and damage to equipment or supplies. These problems require frequent rerunning of a job, error correction, and replacement and repair of equipment and supplies.

Distinguishing between accidental loss and intentional loss is frequently difficult, however. In fact, some reported intentional loss comes from perpetrators discovering and making use of errors that result in their favor. When a loss occurs, data processing employees and managers tend first to blame the computer hardware and the problem becomes

one for the computer vendor maintenance personnel to solve. Although the problem is rarely a hardware error, proof of this fact is usually required before someone searches elsewhere for the source of the loss.

The next most common area of suspicion is the user department or the source of data generation. Next, blame tends to be placed on the computer programming staff. Finally, when all other targets of blame have been exonerated, data processing employees will suspect their own work. Computer operators, programmers, maintenance engineers, and users meet to argue over who should start looking for the cause of a loss in their area. The possibility that it was intentionally caused is even more remote from their thoughts because they assume they function in a benign environment.

People in many computer centers do not yet understand the significant difference between accidental loss from errors and omissions and intentionally caused losses. Organizations using computers have been fighting accidental loss since the beginning of automated data processing. They have anticipated the careless errors that people commit. Well-known solutions are usually effectively applied given the degree of motivation and cost-effectiveness of controls. On the other hand, they anticipate that the same controls used in the same ways will also hinder people engaged in intentional acts that result in losses. They frequently fail to understand that they are dealing with individuals intent on using their skill, knowledge, and access capabilities to solve a problem or reach an illicit goal. This situation presents a much more challenging vulnerability that requires adequate safeguards and controls not yet fully developed or realized, let alone adequately applied.

4. Vulnerabilities from Natural Forces

Computer systems clearly are vulnerable to a wide range of natural as well as man-made forces. Table 20 lists most of the natural forces that can cause damage and destruction. Computer systems and facilities are fragile, and intruders can find great leverage using simple methods to engage in malicious mischief, arson, vandalism, sabotage, and extortion with threats of damage. Intruders can also take advantage of natural events from extreme weather and earth movements to achieve destructive purposes.

In the 1960s, magnetic fields were identified as a major source of potential attacks. Tests performed at the National Bureau of Standards indicated that the erasure of magnetically recorded data on tapes and disks does not pose a significant problem because the field strength of a magnet deteriorates rapidly with distance. A number of alleged crimes in which individuals used magnets to erase massive amounts of magnetically recorded data never actually occurred. A small danger exists that a magnetic tape or disk might be placed near enough to a source of a magnetic field to cause erasure. Such fields could be generated by large electric motors or generators, for example.

One of the few verified cases of use of a magnet to destroy data occurred in a New York City office in 1962[15]. A disgruntled employee used a hand-held magnet against the coiled edge of a magnetic tape through the flange window of the reel. He was successful in erasing one bit position closest to the edge that was used to check errors. The data contents of the tape were still readable, however. A large hand-held magnet would normally have to be placed within a fraction of an inch of the recording surfaces to have a significant impact.

Most computer centers possess a degaussing (demagnetizing) device to erase magnetic tapes. Degaussers should normally be kept under lock and key or at least located in a room or area different from where magnetic tapes may be stored.

Table 20

Natural Forces Causing Losses

Extreme temperature		
Hot weather	Cold weather	Fire
Gas		
War gases	Commercial vapors	Humid air
Steam	Wind	Tornado
Explosions	Smoke	Dust
Liquids		
Water	Rain	Flood
Ice	Snow	Sleet
Hail	Chemical solvents	Fuels
Living organisms		
Viruses	Rodents	People
Bacteria	Insects	Hair
Disease carriers	Wastes	Skin oil
Projectiles		
Bullets	Shrapnel	Powered
Thrown objects	Meteorites	missiles
Vehicles		
Earth movements		
Collapse	Slides	Flows
Liquefaction	Shaking	Waves
Cracking	Separation	Shearing
Electromagnetic discharges		
Electric surges	Electric blackout	Static
Microwaves	Magnetism	electricity
Atomic radiation	Cosmic waves	Lasers

Computers can also be adversely affected by radio frequency energy that might emanate from a radar antenna or other

high energy source. This problem is mitigated by putting a conductive, grounded screening material in the walls around a computer—a Faraday cage.

Under very limited conditions, radio frequency emanations normally produced by a computer system may be monitored by sensitive radio receivers and used for espionage purposes. This can occur only when one piece of computer equipment is sufficiently isolated from all other computer equipment—at least 20 ft or 30 ft away. However, the cost of the monitoring radio receiver and technical skills required make this kind of crime most unlikely except possibly in military systems. Although radio emanations from computer equipment can be successfully monitored up to a mile away from the source, there are much easier ways of obtaining the information, such as deception, impersonation, theft of documents, or search of paper trash. There have been no proven cases of this method being used for criminal purposes in the business sector.

SECTION V: Computer Crime Prosecution

This section is designed to aid investigators and prosecutors in the practical application of technical knowledge of computers to the case development and prosecution of computer crime. It covers legal definitions of technical terms, methods of investigating and obtaining evidence at crime sites, and prosecution techniques. Section VI addresses the applicability of the law to such crime. Because investigators and prosecutors are assumed to already be trained in investigative and prosecution techniques, this section focuses only on those aspects requiring application of computer technology, the computer environment, job responsibilities (including management), computer operation, and security provisions described in previous sections. Appendices E, F, and G are also relevant and should be consulted during perusal of this section.

Prosecutors and investigators can avoid becoming overwhelmed by the complexity of computer technology by applying their knowledge and experience from other types of criminal cases, obtaining only necessary technical information from experts, and translating the technical aspects into terms more familiar to the criminal justice community. The technical aspects should be subordinated to the typical crime facts as much as possible; confusion over technical matters can lead to reasonable doubt and a lost case. In fact, the defendant may be well aware of this point and emphasize the technical complexity.

Several computer crime cases were collected in an American Law Reports annotation of an Indiana case.* Of the 19 cases discussed in that annotation, only one involved prosecution under a computer crime statute, and even there the computer crime was a relatively minor issue. The case was really a rape and capital murder case, in which the accused had used his victim's automatic teller card to withdraw money from her bank account. He was convicted of that and of all other charges.† Eleven case studies illustrating investigative and prosecutorial skills are presented in J. Thomas McEwen's report, "Dedicated Computer Crime Units," National Institute of Justice (1989).

A prosecutor attempting to introduce computer-related evidence in a trial must carefully prove its authenticity and relevance. A technically knowledgeable defense attorney often can effectively prevent the court's acceptance of such evidence, by confusing the court with technical complexity and obscurity or by challenging the integrity of the material or its production. Because the prosecutor may have to match his or her experts with those of the defense, the more knowledgeable and competent experts who have been more directly involved in the evidence-producing processes and who are the more effective witnesses on the stand will prevail[32].

A team approach to a complex computer crime case is desirable. An investigator, a DDA, a computer expert, and an EDP auditor would make an ideal team. The capabilities and roles of experts and auditors are presented in Section III of this manual.

If possible, the investigation should be well advanced before an arrest is made, exhibits obtained, experts consulted, search warrants and affidavits completed, witnesses interrogated, and subpoenas prepared. The investigation might alert the possible perpetrators, allowing them time to obliterate evidence, often an easy task in a computerized environment. This danger must be taken into account in determining the degree, type, and secrecy level of an investigation.

A. Legal Definitions in Computer Technology

Knowledge of computer technology in the law can be useful to prosecutors in considering the various aspects of a computer crime case. The application of this information in case development is discussed below. See the glossary for succinct definitions of technical terms and Section I for the definitions of computer crime and computer-related crime.

One trap prosecutors may face is the challenge to their claim that a computer was involved in an alleged crime that would make a computer crime law applicable. To avoid this trap, the prosecutor should minimize the computer's role and prosecute on the basis of the criminal law most familiar to the prosecutor and the court. For example, theft of a computer program might be prosecuted as a simple copyright law violation. It may not be reasonable to make the case for a program theft that involves the introduction of complex definitions of a computer program and methods of criminally copying it from a computer storage device.

In the preparation of a case deeply involving computer technology, the technical aspects of the case therefore should be carefully identified. This evaluation should include computers and computer programs, if they are

* State v. McGraw, 480 N.E.2d 552, 51 A.L.R.4th 963 (Ind. 1985); Annotation: Criminal liability for theft of, interference with, or unauthorized use of, computer programs, files, or systems, 51 A.L.R.4th 971. This collection is of cases that have been published in official reporting systems, primarily the regional reporters of the West Publishing Company. Undoubtedly, many other cases have no reported opinion of the court.

† State v. Gillies, 135 Ariz. 500, 662 P.2d 1007 (1983), aff'd, 142 Ariz. 564, 691 P.2d 655, cert. den., 105 S.Ct. 1775, 84 L.Ed.2d 834.

involved. Referring to testimony, studies, and supporting or opposing statements made when the law was enacted also may be useful.

1. Definitions of Computers

Consider the range of definitions of computers found in current state and federal laws:

- Florida: "*Computer* means an internally programmed automatic device that performs data processing. *Computer system* means a set of related or connected or unconnected computer equipment, devices, or computer software. *Computer network* means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities."
- Arizona: "*Computer* means an electronic device that performs logical, arithmetic, or memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in the system network. *Computer system* means a set of related connected or unconnected computer equipment, devices, and software. *Computer network* means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals or a complex consisting of two or more interconnected computers."
- California: "*Computer system* means a machine or collection of machines used for governmental, educational, or commercial purposes but excluding pocket calculators that are not programmable or access external files, one or more of which contain computer programs or data that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control. *Computer network* means an interconnection of two or more computer systems."
- Illinois: "*Computer* means an internally programmed, general-purpose digital device capable of automatically accepting data, processing data, and supplying the results of the operation. *Computer system* means a set of related, connected devices including the computer and other devices, including but not limited to data input and output, storage devices, data communications links and computer programs, and data that make the system capable of performing the special-purpose data processing tasks for which it is specified."
- Utah: "*Computer* means any electronic device or communication facility with data processing ability."
- New York: "*Computer* means a device or group of devices which, by manipulation of electronic, magnetic, optical, or electrochemical impulses, pursuant to a computer program can automatically perform arithmetic, logical, storage,or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enable such computer to store, retrieve, or communicate to or from a person, another computer or another device the results of computer operations, computer programs, or computer data."
- Federal: "*Computer* means an electronic magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

Within any of these definitions, a computer or computer system could be a giant IBM 3090 computer system occupying several large rooms or any device containing a microprocessor chip such as a programmable laptop computer or electronic game.

In one definition, a computer must be internally programmed. Historically, the term "internally programmed" has been used to differentiate a computer from a calculator where all of the instructions are manually entered one at a time and would be considered an externally programmed device. However, the algorithm (set of rules) for performing multiplication and division is automatic, containing internally programmed functions that would make a calculator internally programmed as well.

Another definition of this term might be that the computer program must be generated internally in the device rather than the typical process of writing computer programs on coding forms, keying them into computer media, entering them into the device, and starting the device to follow the instructions in the program. Under this interpretation, no devices could be defined as a computer except those that automatically generate their own computer programs—a highly unlikely possibility in today's technology. Some computers have been programmed to be self-learning (heuristic) and construct their own programs to solve problems in a field known as artificial intelligence. However, the programs that perform the self-learning have been written externally and placed in the computer.

Conceivably, charges in an alleged crime may refer to computer when computer system or computer network is

meant, or it could refer to computer system when only an isolated computer is involved. The federal law uses the generic term computer and ignores the computer system and computer network terms. Therefore, defendants must be charged carefully to match the definitions of computer and computer system.

Other problems appear when computer is defined as an electronic device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses. Some may argue that a word processor system does not perform logical, arithmetic, or memory functions but performs functions on words and symbols, storing them in a device not covered by the term "memory functions." The definition also incorporates all communication facilities that are connected or related to such a device in a system or network. If a computer is on-line to the dial-up telephone system, then every telephone system and every computer connected to the telephone system become part of the computer. These definitions are so broad as to make the law so unspecific that it becomes meaningless.

Some of the definitions include software or computer programs among the parts of a computer system or computer. In most cases, computer programs (using the less ambiguous term) are not considered a part of the computer, but are entered or called on from an external storage device only when data processing is to be performed. Some more advanced computers have permanently installed computer programs, and others have computer programs semipermanently installed (sometimes referred to as firmware). The meaning of software and programs may be differentiated between the computer operating system programs that normally must be present in a large-scale computer to make it function on a practical basis and application programs that perform problem solving and are served by the operating system. However, this distinction is not made in the definitions.

The definition of a computer in the California statute states that a machine or collection of machines is a computer system only if it is used for governmental, educational, or commercial purposes, thereby excluding or including computer systems based on their use. A computer owned by an individual and used as a hobby or for amusement would not be covered by the statute, whereas the same computer, if used by a small business, would be covered.

2. Definitions of Computer Programs

Computer programs have been defined in the various state statutes as follows:

- Florida: "*Computer program* means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data. *Computer software* means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system."
- Arizona: "*Computer program* means a series of instructions or statements in a form acceptable to a computer which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer systems."
- California: "*Computer program* means an ordered set of instructions or statements or related data that when automatically executed in actual or modified form in a computer system, causes it to perform specified functions."
- Illinois: "*Computer program* means a series of coded instructions or statements in a form acceptable to a computer which causes the computer to process data in order to achieve a certain result."
- New York: "*Computer program* is property and means an ordered set of data representing coded instructions or statements that, when executed by computer, cause the computer to process data or direct the computer to perform one or more computer operations or both and may be in any form including magnetic storage media, punched cards, or stored internally in the memory of the computer."

The term "computer software" is jargon. Software sometimes refers to a computer operating system; at other times it refers to any computer program; and sometimes, as in the previous definitions, it includes the documentation, which may mean computer user manuals, specifications, input data to the program, and output from the use of the program.

A computer program is often viewed as only computer instructions. Yet, computer programs often contain considerable amounts of data that are used as constants, tables, or parameters. According to some definitions, when a program is executed by a computer, it causes the computer to process the data. Computer programs can be written and used that do not process data but only perform some logical function, such as setting electronic switches. Some computer programs look like ordinary English language text; other computer programs can be written as nonsequential graphical diagrams or tables of data in high-level languages such as spread sheet applications.

The federal statute does not use or define the terms program or software but substitutes the "use of a computer" for "execution of a program." It also includes a program as information in a computer when a program may be the object of attack or tool for fraud.

B. Computer Evidence Considerations

As in the preparation of any case for prosecution, the use of evidence is a significant element. The most likely of the principal defense strategies to arise in a computer crime case is an attack on the admissibility of the prosecutor's computer or computer-generated physical evidence. The prosecutor should be alerted that perhaps in no other type of crime is an attack on admissibility of evidence more likely to succeed. The purpose of the following subsections is to alert prosecutors and investigators to those potential evidence issues based on general legal principles that are most likely to be used in computer crime cases.

1. Search and Seizure

The nature of computer crime investigation frequently requires a search of a computer center or a remote computer terminal location, either as the situs of the crime or of the fruits of the crime. Equally likely is the necessity to seize computer or computer-generated physical evidence for successful prosecution.

Thus, an entire Pandora's box of legal issues becomes available to the defense. The nemesis here is the exclusionary rule that could well obliterate the prosecutor's case. Most search and seizure issues, such as consent, informers, entry, and searches incident to detention and arrest, generally apply much as they would in noncomputer cases.

In computer crime cases, search warrants should generally be obtained and used. Examples of computer crime search warrants are found in two companion reports cited in the preface of this manual. The plain view doctrine should be cautiously relied on. The defense will likely attempt to show the lack of sophistication of most prosecutors and investigators in computer technology.

The use of an expert informant at the search scene to indicate the items to be seized should not be relied on, however. [California prosecutors are directed to *People* vs. *Superior Court* (Williams) 77 C.A. 3d 69 on page 78 for a discussion of this issue.] Informers are generally insiders and legally "untested" or "unreliable." Thus, their information should be corroborated before the warrant is prepared.

A difficult problem in drafting computer-related search warrants is the tightrope walk between "reasonable particularity" in describing the items to be seized. Seizing items not described in the warrant should be avoided as much as possible. A data processing expert can assist in drafting the warrant to ensure that all pertinent system hardware and program components are included.

The timeliness of the execution of the warrant may also be critical. Evidence of an operational fraud—that is, a fraud that occurs only during an actual computer operation—is timely by definition. However, the problem becomes more difficult when the operational fraud arises out of irregular computer usage.

Many more search and seizure traps may await the computer crime prosecutor. Therefore, imagination and ingenuity are critical, as are the training and experience obtained in all computer search and seizure situations.

2. Obtaining Evidence

Obtaining documents in a search is comparatively easy; they can be visually identified, and computer technology expertise is not usually needed. Documents such as system manuals, computer run books, program documentation, logs, data and program input forms, and computer-printed forms are typically labeled. Whether they are complete, originals, or copies can be determined by questioning document custodians.

Requesting certain program documentation may require knowledge of computer program concepts to identify the types and extent of documentation required (e.g., source listing, object listing, flowcharts, test data, storage dumps). (Note, however, that program documentation is frequently obsolete.) Although program documentation is usually found in a centralized library, individual programmers in some organizations hold the most recent documentation. If questions arise about what may be obtained or identified, an expert should accompany the search officer.

Taking possession of other computer media materials may be more technically complex. Magnetic tapes, cartridges, and disks are normally externally labeled, but a log or program documentation may be necessary to obtain full titles or descriptions. The program documentation must be for the program that produces or uses the content of the tape or disk. Moreover, a large tape or disk file may reside on more than one reel or cartridge of tape (called volumes). A trusted technologist may need to check the contents of a tape or disk (without changing them) by using a compatible computer and computer program.

Searching for information inside a computer can be highly complex and requires experts. Preparing a search warrant for this task is also complex and requires expert advice. Any materials that must be seized may also be required for continued operation of the computer center. If the intent is not to inhibit continued operation, the material may have to be copied. If the copying is to be done at the searched facilities, a trusted person should be assigned to the task. Information can be destroyed before it is removed; however, if it is destroyed in a computer center, backup copies are frequently stored locally in a media library or at a remote facility. Note that computer usage logs and operator instructions are now often stored on disk and viewed on console screens rather than printed on paper. They would have to be printed separately to carry a record

away. Appendix E describes additional tools for examining the contents of computers.

The California Evidence Code now states that computer-generated evidence is the same as traditional evidence. However, the reliability and integrity of the computer-generated evidence must be proved. Computer-generated evidence can be the result of the work of several different technologists, including:

- Systems analysts who designed and specified the computer program that produced the evidence
- Programmers who wrote and tested the programs
- Computer operators who operated the computer to run the programs that produced the report
- Data preparations staff who prepared the data in computer-readable form (tape or disk)
- Tape librarians with the responsibility for supplying the correct tapes or disks containing the source data
- Electronic maintenance engineers who maintain correct function of the hardware
- Job setup clerks and job output clerks who are responsible for manual handling of the input and output before and after the job is run
- System maintenance programmers responsible for the integrity of the computer operating system used in the execution of the computer program
- End users who supply input data, authorize execution of the computer program, and use the results.

Using a generally known, accepted, and widely used computer program package as evidence is better than using a special-purpose program. Generalized EDP audit packages are available from several program vendors and CPA firms (see Appendix E). These programs should be used whenever possible to examine and print the contents of computer media. Logs and journals that provide records of program execution should be obtained and initialed by the individuals responsible for the actions that result in these records.

The efforts used to safeguard the hardware, software, and data can be an important aspect of the investigation and prosecution of a suspected computer crime. A security specialist at an organization can provide information on deviations from normal activities that might be associated with a suspected crime. The specialist's records could provide significant amounts of evidence that might be used in a criminal trial, primarily because they may be an exception to hearsay evidence rules; the records will frequently be produced in the normal course of business. The computer security specialist can quickly and easily brief an investigator or prosecutor on the safeguards that may be associated with or violated in a computer crime.

A computer security office may have or be able to obtain some of the following information files of use to the investigator:

- Security review and recommendation reports.
- Audit reports filed by date and subject that could reveal vulnerabilities and problems.
- Computer operations exception reports of checkpoint restarts, missing tapes and output, data communications traffic errors, password and access failures, and automatic dial-back exception records.
- Loss experience reports of accidental and intentional acts.
- Lists of assets including all computer equipment and programs, data files, supplies, and facilities.
- Derogatory or sensitive information published about the organization such as in hacker bulletin boards.
- Floor plans of all facilities.
- Diagrams of equipment connections.
- Network configuration.
- Maintenance records of safeguards and controls.
- Enrolled computer users summary files and listings.

Investigators may have a problem, however, in convincing a victim to relinquish important evidence in the form of magnetic tape reels or cartridges, disk packs, or diskettes of master files and various materials needed to continue the business. This problem might easily be solved by having the victim use copies of the required material. The investigator must be given the original material properly marked and inventoried and not the copy; otherwise, the integrity of the copying would have to be established.

The EDP auditor within the victimized organization or from the external CPA organization that audits the victimized organization can be particularly helpful. As stated in Section III, their function is to ensure the integrity of all data processing for victimized organizations. The professional societies (Institute of Internal Auditors, EDP Auditors Association, Information Systems Security Association, and the American Institute of CPAs) to which these auditors belong often have certification programs and codes of ethics that may be used to assist in validating the trustworthiness of any auditors who may be needed.

Much can be gained from the negative experiences and complications of obtaining and introducing computer-related evidence in trials. These experiences often spotlight the kinds of additional controls and safeguards that potential victims of computer crime should install. Examples of safeguards are the labeling of computer programs and data, journaling of computer system activity, audit trails built into systems that result in reports that can be categorized

as ordinary business reports, and retention of potential evidence for a reasonable period of time.

3. Personal Computer Crime Investigation

This section as well as Appendices F and G focus on criminal investigations that involve personal computer systems and their use for intrusion into other computers. Police have mastered investigative techniques to identify, arrest, and convict criminals committing routine types of crime, but not usually for electronic crimes, specifically ones involving personal computers. Investigators and prosecutors should start working with a computer intrusion victim as early as possible, especially given that intrusion may last for days or even months. Appendix F provides detailed guidelines for victims working with investigators to deal with computer intrusions that are facilitated by personal computers. This appendix shows the extent of and close working relationship needed between victims, investigators, and prosecutors. Appendix G provides a detailed, step-by-step guide to conducting an on-site investigation and search of a personal computer facility. It describes investigative techniques, supplies needed to execute a search, the approach to a target system, use of DNR telephone equipment, and computer dismantling and reassembling.

Physical evidence still must be identified and collected. In personal computer fraud, physical evidence takes many forms including sales invoices, computer printouts, handwritten notes, photographs, fingerprints, computer audit trails, telephone toll records, pen register records, and wire intercept transcripts. Conventional investigative techniques such as surveillances, use of informants, and interviews of witnesses and suspects still apply.

The cost of developing expertise in each type of commercially available personal computer is prohibitive. Thus, criminal justice agencies and departments are caught between wanting to aggressively bring computer criminals to justice and not having sufficient funds to train personnel in the continually changing medium of computer technology.

The greatest challenge in computer crime investigations involves executing a search warrant and reviewing seized computer evidence. Some law enforcement agencies take advantage of "in-house" expertise. Many law enforcement officers are knowledgeable about home computer systems (e.g., Commodore 64, Tandy TRS 80, Apple IIe, IBM compatibles). The officer experienced in a particular system could be particularly helpful in the search, seizure, and subsequent review of computer-related evidence.

The investigators of a computer crime should take the time to identify the magnitude of the case and develop the evidence to support a good conviction. One of the most valuable investigative techniques involves the use of a pen register or dialed-number recorder (DNR). Hackers frequently use stolen long-distance access codes to communicate with associates and intrude on computers. The use of a pen register in concert with review of telephone toll records quickly documents a criminal violation easily provable in court. This technique combined with other conventional investigative tools enhances an investigator's ability to establish that a given suspect did commit the computer crime.

Taking the time to conduct a thorough investigation will identify coconspirators and potential suspects. All too often the underground computer networks and electronic builetin boards alert coconspirators to the "crashing" of a hacker as a result of a search and seizure. Realizing that some hacker investigations could last a long time, investigators evaluate the likely deterrence of a particular course of action versus the benefits of continued investigation.

Understandably, some personal computer crimes necessitate immediate action; the luxury of developing a case methodically and deliberately, using a variety of investigative techniques, is not always an option. When the search is executed, the investigator must pursue each personal computer site independently of others. Appendix G describes the advance preparations for a search and actual search procedures, while Appendix H presents some time-sharing usage examples.

4. Computer Reports as Evidence

Data contained in the storage devices of a computer or in computer-readable media such as magnetic tape, hard or removable disks, or electronic attachable storage devices are sometimes needed as evidence in human-readable form (punch cards are directly readable by humans). Printing on paper or displaying the data on a screen does not normally result in erasing or destroying the data in the computer or computer-readable media unless that is the intended purpose. However, the data in the storage device or media can be erased, replaced with other data, hidden, encrypted, modified, misnamed, misrepresented, physically destroyed, or otherwise made unusable. Normally, only copies of the desired data are obtained.

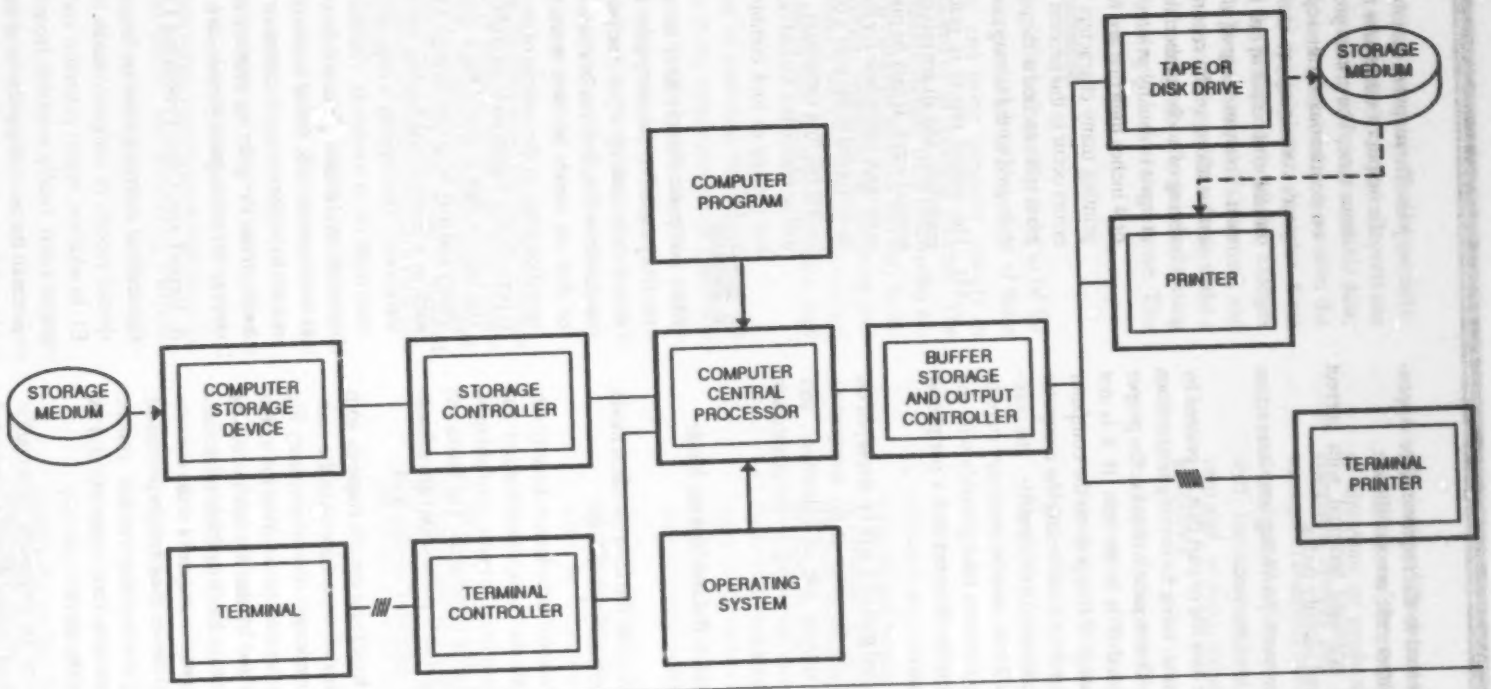
The report production process is summarized in Figure 2. Occupations of people who participate in real-time and nonreal-time modes in the production of a report are also indicated. (Detailed job descriptions are provided in Appendix D.)

a. Production Steps in an On-line System Mode

In an on-line system, printed output can be obtained in two ways: produced at a terminal with an attached printer, or requested from a terminal but printed at the computer site

Figure 2

PRODUCTION PROCESS FOR COMPUTER REPORTS



REAL-TIME PERSONNEL	MEDIA LIBRARIAN	PERIPHERAL OPERATOR	JOB SETUP CLERK	COMPUTER OPERATOR	PERIPHERAL OPERATOR	JOB OUTPUT CLERK	TERMINAL OPERATOR MESSENGER
NONREAL-TIME PERSONNEL	EQUIPMENT MANUFACTURING WORKERS	INSTALLERS TRANSPORTERS	FACILITIES ENGINEERS	MAINTENANCE ENGINEERS	SYSTEM PROGRAMMER	APPLICATION PROGRAMMER	AUDITOR SECURITY SPECIALIST

or elsewhere and delivered to the requester (see Appendix H). The steps in either case are as follows:

(1) Log on to an activated terminal with correct authorization and identity codes.

(2) Enter the system mode providing user interaction with the data file of interest.

(3) Request that the data file or part of it be printed by specifying its name, using formatting instructions and commands. The request will cause the proper file to be accessed if it is on line. If it is not available, a message will appear on the computer console printer or screen informing the computer operator of a request for an off-line file. The computer operator will then take the necessary steps to make the file available on line, possibly with the assistance of a media librarian and a peripheral equipment operator.

(4) The file or a selected part of it will be displayed on a screen, printed on a printer at the terminal or printed at the computer site or elsewhere, and delivered to the user according to the commands entered at the terminal.

b. Production Steps in an Off-Line System Mode (Batch Processing)

In a system where data are to be retrieved in batch mode, the following steps are normally performed:

(1) The user fills out a form to be keyed directly into the computer with the user identification and authorization information, file name, formatting instructions, and retrieval commands. The forms and file media (if in the user's possession) are submitted as a job at the computer service desk.

(2) The job setup clerk delivers the job requests with file media or file media request forms to the computer operator. The operator obtains necessary file media such as tapes or disk packs from the media librarian as authorized by the file media request forms and mounts the media on a peripheral device. The operator then enters commands at the console of the computer that causes the job to be processed consecutively but sharing the various system resources asynchronously (not consecutively) as needed to complete the work.

(3) The report containing the requested information comes from the output printer directly connected to the computer or is produced and stored on a tape or disk storage device for off-line printing. The on-line printing may be performed in a spooling mode where the output is saved on tape or disk and printed later in parallel with computer processing of other jobs. The output of the job usually is combined with the output of other jobs run at approximately the same time. The printer produces the printed reports on continuous forms separated by one or more pages containing job identification, showing termination of output of one job and the starting of the next. To ensure ease of identification, separation, and stacking of the reports, the information consisting of a job number assigned by the computer at input is usually printed in large block letters 3 or 4 inches high that are formed graphically from printing many characters in patterns. Occasional errors occur in this process where the report for one job is still attached to the report for another job and delivered to the wrong user.

(4) The output report is placed with the job input materials, and all are returned to the user in one of several ways. It may be placed on an open shelf or in an open cubby hole for the user to pick up. It may be delivered to the user's office or an intermediate pickup site by a messenger. Sometimes the material will be placed in a locked cabinet for which the user has the key or lock combination.

c. Backup

Most computer centers have an automatic backup and recovery capability for many jobs. If reports or computer-stored data used by a job are inadvertently destroyed, modified, or lost, they can be restored. The tape, cartridge, or disk on which the data were placed is saved for a specified time, or the content of on-line computer storage is periodically copied on to an archive backup tape or disk. The tape or disk is stored for a specified time in a media library and may be cycled through a remote backup facility, such as a commercial backup storage facility, vault, or warehouse. The copying is done after each job or possibly each night or on weekends. Another backup method is to microfilm and archive reports following similar procedures as with tape and disk. Other copies of the data file may also remain in buffer storage locations or on temporary storage media from the printing process until other use of the storage for subsequent jobs occurs.

d. Report and Copy-Producing Computer Programs

Generalized audit programs are frequently used to produce special reports or computer media copies (see Appendix E). In addition, report generator and copying utility programs are normally available from within the operating system in the main computer or at the terminal. The data selected by naming the files, records, and fields may be sorted into various sequences, reordered, and labeled in the required report or media formats. Data may be coded, formatted, and printed or copied in any form desired; however, if available programs do not meet a specific need, a special program must be developed. Programmers often

dislike this type of work and resist requests for specialized output reports or say that it cannot be done. Reports can be obtained, however, from any computer-readable data, in any format desired, in any desired order within the printer line length, line spacing, and character fonts available according to the printer used. All that changes is the size of effort, the programmer skills required, and the cost. The best way to conserve evidence is to make a "bit-mapped" copy of the original computer media using a special utility program available for this purpose. This technique produces an exact copy.

e. Secure Report Production

Although the following instructions may seem to be far more elaborate than is practical, anything short of these methods in obtaining and using computer reports as evidence could be attacked by an opposing attorney. The only alternative is to obtain testimony from trustworthy experts to support the less elaborate methods that may be used. Two tasks are required, each using the following procedures, the first to make a working copy of the original evidence and the second to print the report from the copy made.

Errors and omissions or malicious intentional acts are possible at each stage in the report-producing process or by nonreal-time program or data modification (e.g., by using the Trojan horse or superzapping techniques). Preventing or detecting sufficiently sophisticated intentional acts is often not possible on a practical basis. Therefore, varying degrees of precautions must be taken.

Copying and printing the contents of the storage medium (tape or disk) in one or more different computer centers is advisable. In addition, personnel in another center should have no special interest in the work they would be required to do. The primary concern is to determine that a valid data source has been obtained.

The most elaborate security and integrity can be ensured by following the steps listed below. The steps require that a trusted computer user and one or more observers competent in all applicable technical subjects and equipment used be identified. A handwritten log should be prepared describing each action taken, naming personnel involved, recording times and places, and identifying materials, names, and serial numbers of all equipment, computer programs used, and all results.

(1) Preparing the job for submission to the computer system requires obtaining the correct data source medium (tape, disk, or storage device), a test data file in the same type of medium with a human-readable copy of the data, a trusted computer printing or copying program, a trusted computer operating system, and a trusted computer system. Potential threats to the integrity of the effort include substitution of the data or test sources, Trojan horse modification of the program or operating system, or electronic or mechanical modification of the computer system (see Section II). A trusted manager of computer operations should be required to perform all actions or personally direct his or her staff. The data storage medium, if removable (tape, cartridge, or disk), should be positively identified as follows:

- Tape: Serial number usually in large block characters affixed by the computer center in which it was first used; tape reel or cartridge label affixed to the side or flange of the reel identifying (possibly in encoded form) the current contents of the tape and usually a date on which the tape was last certified or tested; and an internal label with equivalent content identification and reel or cartridge number recorded as the tape header or first record on the tape. A computer program must be executed on a computer to determine the content of the internal label or header.
- Disk: External labels are similar to those for tapes. Internal labels are normally recorded at the beginning of each file of data and in the file directory on the disk or each cylinder or sector.
- On-line storage: There is no way to visually identify the data directly. They can only be identified by executing a computer program that causes the identification to be printed or displayed from a file directory.

A trusted individual who knows about the data source should verify the identity of the data and initial the input storage medium on the external label and do the same for the output medium in the first task of copying. He or she should also observe the safekeeping of the media and their usage, being aware that tape can be spliced, magnetically modified, and wound onto a different reel and a disk can be placed in a different cover or magnetically modified. Determining the integrity of data in on-line storage is impractical, unless previously encrypted with an encryption key kept confidential from anyone who would pose a threat. The only assurance of integrity is the trustworthiness of all persons with the skills, knowledge, and access to modify the on-line data. This also holds true for removable media, once placed on a computer system storage device.

When the computer copying or printer program is in a removable medium, a trusted individual should identify it. The program should be obtained from an independent source where it would be

reasonably free from tampering by any parties to the crime under investigation. The copy of the operating system and related utility programs should be obtained in the same way. A program and operating system already in on-line computer storage should not be used, unless completely normal processing prior to the task can be verified.

The job set-up process should be observed by the appropriate technical expert. All documents and new data storage media for job input and output purposes should be logged and initialed by the person supplying and using them.

The integrity of the program, operating system, and computer system cannot be ensured on a practical basis because they are too large and complex. The capability to prove the correctness of the performance of a program or a computer is a continuing subject for research. Therefore, total trust must be placed in the technologists and vendors who designed, implemented, operate, and maintain the products. The more widely used a product and the more reputable the vendor, the greater the likelihood of its integrity; nevertheless, it takes only one individual with sufficient skills, knowledge, and access to secretly modify it[33, 34].

Actions can be taken to partially compensate for this vulnerability. If the computer design engineers and maintenance programmers are available, they can be consulted and their trustworthiness evaluated. It may also be possible to document the care taken in the design and implementation of the products used. Experts and state-of-the-art literature can be used to evaluate and establish reasonable care. Other users of the same products can also aid in determining the trustworthiness of the products. Copies of the products can also be independently obtained and compared with products used. Finally, the products can be tested as described below.

(2) In the report production steps that involve computer use, the first task is to reduce both the computer system equipment and the computer programs to the practical minimum necessary. This task may be costly in a large computer system because it requires paying for the entire system rather than sharing it with other users. Working on a night or weekend could help reduce cost and the number of users sharing the system. Next, as much residual data and programs as possible should be erased from the system, which is usually too costly for large, secondary storage devices. After the operating system and copying or printer program are refreshed (booted) in storage from the source or backup storage medium, the copy or report producing job can be run using the test data for which the human-readable version is available. The resulting computer media copy or output report can then be checked to assist in ensuring the integrity of the process and the job run under expert observation with the subject data to produce the desired output. The job should be run a second time to compare the results.

(3) Independent, trustworthy observers with the skills and knowledge to determine correct operations should observe all production steps. Each person involved in producing the report should be identified and should initial the documentation of the materials used and records produced. Copies of all handwritten logs, journals, and computer-produced documents, including the computer console log, should be collected.

(4) The information in the computer-produced media copy or report should be evaluated for reasonableness. All materials should be carefully preserved and data storage media kept in proper environments (within heat and humidity constraints).

5. Caring for Evidence

Some types of computer-related evidence require special care. Storage environments must be controlled, and physical damage from manual handling must be avoided. Criminal justice agencies normally have evidence storage and archiving facilities, but these environments may not be suited to computer evidence and correct handling experience may be lacking. Consult Appendix G for the context in which evidence is gathered. The special needs of various types of evidence are described below:

- Magnetic tape and magnetic disk

  Storage: 40-90 °F, 20-80% relative humidity (80 °F Wet Bulb Max). The storage life for normal data retention and recovery is 2 years. Longer storage periods may necessitate production of new, verified copies or special equipment to read the media (consult the manufacturer of the media for advice).

  Handling: Store, handle, and transport items in hard cover containers. Avoid dropping or squeezing them. Always grasp tape reels by the hub; do not touch, bend, or crease any part of the recording surface (except the first 5 ft or leader of tape). Avoid placing items near strong magnetic fields that might be created by a motor or permanent magnet. Affix tags or marks on containers or reel surfaces that do not come in contact with tape or disk drive equipment. Store tape reels vertically in tape storage racks and disks on flat wide shelves.

- Punch cards and punch paper tape

  Although punch cards and punch paper tape are no longer used in modern data processing, information may still exist in these media, and very old records may be important evidence. Therefore, advice on handling them is provided here.

  Storage: Same as magnetic tape. Storage life indefinite.

  Handling: Avoid folding, spinning, or knicking edges. Never use paper clips or rubber bands. Store in the metal or cardboard boxes in which they come from the manufacturer. Store under mild pressure (in full boxes) to avoid warping. Jog card decks to align them on a jog table (on top of card equipment). Wind paper tape on tape winders only (some tape is accordian folded). Individual cards and pieces of tape can be handled manually, with care not to damage edges. Tagging or marking methods are not critical. Avoid tape that removes paper surfaces or covers punched holes.

- Computer listings

  Storage: No restrictions except to avoid strong light to reduce fading. Store on flat surfaces between covers (binders).

  Handling: Continuous forms should be burst into separate pages for ease in reading, but not burst if the continuous form nature of the listing is important to the case. Check for page sequence or numbering. Some printers use special paper that may require special handling for preservation. (Consult the manufacturer for advice.) There are no tagging or marking restrictions.

- Electronic and mechanical components

  Storage and handling: Consult the manufacturer or owner for special instructions.

The owners of computer-related evidence may have special problems when the evidence is removed from their possession or custodianship. The material may be necessary for continuing their legitimate business or other activities. In such cases, the material should be copied in an appropriate, independent, and secure fashion as previously described and the *copy* returned to the rightful owner or user.

6. Privacy and Secrecy of Evidence

Evidence seized in the form of computer media may have data stored that are immaterial to the investigation but that may be confidential to the rightful owner. The existence of such data could involve personal privacy, trade secrets, or government secrets. The problem may be solvable by retrieving and copying on another computer medium only the data at issue in the case. If the data cannot be separated, assurances must be given that the extraneous data will not be revealed and will be stored at least as securely as where it was originally found.

Search and seizure right to privacy issues that arise should be addressed with the same principles as in noncomputer abuse cases. As discussed earlier, the prosecutor should remain alert to these issues; again, taking preventive measures during search and seizure efforts is important.

Other search and seizure right to privacy issues may arise where personal, privileged, or classified information or transactions are involved. Obtaining consent from the individual(s) who are the subjects of the information is sometimes feasible.

Even when consent is not obtained, sufficient safeguards are available in most jurisdictions to minimize this problem. A hearing outside the presence of the jury or even an "in camera" hearing may allow the court to overrule the objection or perhaps excise the specific objectionable portions. With the exercise of such safeguards, the compelling state interest in law enforcement will generally prevail.

7. Conjectural Forensics

Several conjectural forms of evidence in computer technology that are not yet tested in the courts may become important:

- Can a magnetic or optical digital recording be proven to have been written by a particular disk or tape drive? This finding could associate a possessor of media with a computer on which the media was used. Magnetic media manufacturers have elaborate testing equipment that may resolve such questions.
- Can the magnetic strength or track alignment of part of a recording be compared to another or adjacent part of a recording and be shown to have been written at a different time? This finding might be used to show that the name or last write date of a file in a disk directory was changed, and a document was falsified.
- Under what circumstances could a digital signature be uniquely identified with a person? A person could deny exclusive knowledge of a secret key or claim a coincidence of identical signature. This finding will be increasingly important as electronic data interchange (EDI) advances.
- Under what circumstances will biometric authentication of the identity of computer and remote terminal computer users be accepted? Biometric products include voice analysis, fingerprint scanning, hand

shape measurements, retinal eye scanning, and keyboard keying rhythms. False acceptance and false rejection error rates are being lowered from 1.0 to 0.001%.

- To what extent will the combination of secret password knowledge, possession of a uniquely coded token (e.g., smart card), and a biometric measurement be accepted as valid authentication of a person's identity?

C. Prosecution

The discussion in this section introduces technical and legal considerations, as well as practical information on trial tactics. Some portions have not been updated since 1979 but are still valid.

1. Foundational Problems

Generally, before proffered physical evidence can be admitted into evidence, the prosecutor must prove certain "preliminary facts." These preliminary facts are to be contrasted with the facts sought to be proved by the evidence. Quite obviously, a principal defense tactic will be to attack admissibility based on foundational issues, an attack to which the prosecutor is particularly vulnerable.

a. Authentication

Authentication of a written statement generally means introducing evidence sufficient to sustain a finding or establishing by other means that the written statement is in fact the writing the proponent of the evidence claims it is. Thus, the prosecutor will need testimony from someone who can verify that the purported maker of the item—namely, the particular computer system that generated the proffered item—is the actual maker. Note that the proponent of a writing satisfies his burden of establishing the preliminary fact of authentication by introducing evidence that is sufficient for a trier of fact to reasonably find that the proffered item is what the proponent claims. Hence, it is critical at this stage not to claim more than simply the output process—that is, that the proffered item was generated by such-and-such computer at such-and-such place and time, and nothing more.

Prosecutors significantly compound the authentication problem if they attempt at this point to claim that the proffered item reflects a particular configuration or programmed process internally within the computer, or that it reflects particular information fed earlier into the computer. To do so would allow the defense to raise objections based on the authentication of such specific internal configuration or earlier input. These defense objections would be valid because the extended "claim" infers that the proffered item is merely a copy of secondary evidence of something else. Thus, the "original" writing—namely, again either the internal configuration or the earlier input—would have to first be authenticated in addition to authentication of the secondary evidence. These matters would be addressed under the Best Evidence and Hearsay-Business Record Exception rules, and there is certainly no need to compound the difficulty.

b. Best Evidence Rule

Computers operate by use of electronic and magnetic pulses and states or laser-reflecting spots not visible to the human eye. Because the law requires that triers of facts be human beings, with human eyes, secondary evidence in the form of computer-generated physical printed matter, purporting to be a copy of the electronic signals, will often be essential to successful prosecution.

Thus, the formidable problem of the best evidence rule arises for the prosecutor of computer crime. Accuracy will need to be foundationally shown. The Federal Rules of Evidence and Rule 255 of the California Evidence Code deem proffered computer-generated evidence to be an "original" on a showing of accuracy, or in a "copy" jurisdiction where traditional foundational findings are required.

In actuality, the problem is double-barreled. Not only must the court be satisfied that the showing of accuracy has been sufficient to permit the item to be submitted to the trier of fact, but also the trier of fact must independently be persuaded beyond a reasonable doubt on the weight of the evidence that the item is accurate.

The defense will have available EDP experts who can testify as to the unreliability of computers and the possibility of either hardware or program error at virtually every stage in the computer process, including the output generation components through which the proffered evidence was derived. Expert opinion is so plentiful that, based only on general technological probabilities, much less the specific system at issue, the prosecutor's secondary evidence fails the legal standard of accuracy required.

An important caveat to the unsuspecting investigator or prosecutor is *not* to assume that the documentation of a computer program is an accurate reflection of the actual program in operation at the time of an alleged crime. In most system development projects, the documentation is typically a last-minute, low-priority effort, often incomplete, and frequently not updated to reflect program changes made since the program has become operational. Unless the documentation has been recently verified, any specific portion of a program should be used cautiously and never offered as evidence in court unless specifically verified immediately beforehand.

A solution to these problems is to select potential witnesses who not only are experts in the general state of the art, but

also have expert familiarity with the computer operations or programming where the offense occurred. These witnesses should be sought out as early as possible so as to use their knowledge as a resource in determining preventive action when obtaining physical evidence as well as to discuss their testimony. Appendix I lists directories and data bases for contacting expert witnesses.

2. Proprietary Rights of Computer Programs

The prosecutor must first know the differences among the various forms a computer program takes to establish ownership. The program will usually be in source code form, the language in which the programmer wrote it. Assembly code form is the symbolic language that the computer system sometimes uses as an intermediate form to translate the program into actual machine code that the computer executes. Source code programs often will be executed directly in a computer where the lower, more detailed forms of the programs are immaterial to the execution of the program so long as the internal language translators have an acceptable level of integrity. Therefore, only the source code version of the program and its input and output need be considered. The integrity of the intermediate forms and processing could be established through expert witnesses.

Not all computer programs are physically labeled as to their ownership. Commercial program packages may have adequate labels in terms of copyright and trade secret law. Sometimes these packages have secret-coded labels inserted or buried within the program itself—much like a map maker will put a fictitious name on a map to show ownership. No two nontrivial programs written by different people are ever identical, even though their function may be identical. Computer programs even in higher level languages are generally unintelligible to the layman; however, many computer programs are extensively annotated line by line in easy-to-read English that the layman may understand.

Many of these computer programs and computer data have significant value to their owners. Furthermore, much of the information may be highly sensitive to a business, particularly if it is revealed in open court. The most common and most effective protection of such information is under trade secret laws. Most computer programs that are licensed for use by service bureaus, time-sharing companies, computer vendors, and program vendors are protected as trade secrets and often only their use and not copies are licensed to the customers using these programs.

Demonstration that proprietary information is a trade secret has typically been straightforward, and precedents for these traditional areas are well established. However, increasing numbers of assets in the form of data and computer programs that may constitute trade secrets are stored in computers and computer media, and few precedents exist.

A trade secret must be adequately protected. As stated earlier, computer programs are commonly protected as trade secrets and licensed for use by others. The patents on some computer programs have been mainly for processes embodied in electronic circuitry. The U.S. Supreme Court has ruled on three occasions that specific programs were not patentable. Although programs are copyrightable, protection is of minimal value because it protects only the expression of the idea but not the idea itself. Trade secrets may include data that represent secret processes, product specifications, geologic information, business records, or customer lists.

The first step in determining that adequate protection has been applied to qualify data or computer programs as trade secrets is to identify all copies, representations, forms, locations, and custodians of such assets. Most data and programs stored in a computer or computer media also exist in other forms and locations. In computer-using organizations, the computer users, the computer services supplier, and the data processing organization sometimes disagree over the custody and responsibility for the security of the trade secret. This dispute is usually resolved by finding that each is responsible for the forms of the material in their respective domains. However, the data processing organization may claim that it cannot always be aware of the secret nature of the material among the high volumes of data and programs in its domain. This problem is especially acute in on-line computer systems where the users control their own data and programs through terminals. In batch-operated systems, the point at which custodianship of a job submitted for computer processing or job output passes from one area to the other, is sometimes unclear.

Proof of adequate security for a trade secret consists of the combination of all safeguards and controls of all forms of the secret and the basis on which it may be offered for use by others. In one case (*Ward* vs. *California*, *1972*) of theft of a computer program from the storage of a computer over a telephone line, the following safeguards and controls were accepted as adequate (but may not be adequate under current practices):

- Secret accounting number needed for terminal access.
- Secret site code number needed for terminal access.
- Unlisted telephone number of access to the computer.

best copy available

- Secret file name in which the computer program was stored.
- Restricted use of the program by others and no copies of the program given out. (The program was a utility program available only for use in the time-sharing computer.)
- Awareness of data processing employees of the proprietary nature of the program.

Several inadvertent disclosures of the program were noted but did not constitute loss of trade secret status. The defense counsel contested whether a theft had even occurred. An expert witness stated that it was his practice (although not an industry standard) that any program or data he could obtain from a commercially available time-sharing service through a terminal was by definition in the public domain if no proprietary notice was given. This Peninsula ethic, so called because the individual resides on the San Francisco Peninsula, is not a generally accepted concept, but it shows the lack of concurrence on generally accepted practices.

3. Evidentiary Problems with Computer Records

As a written statement, computer-generated printed evidence offered to prove the truth of the matter asserted must satisfy the business record exception requirements before being admissible as a hearsay exception. These requirements are designed to establish the reliability and trustworthiness of such written statements. Here again the prosecutor faces the burden of showing computer reliability, an area fraught with complex technological issues. More than ever, the best prosecutorial strategy is to lead the presumably nontechnical court to focus on the legal issues rather than getting lost in a technical quagmire. The prosecutor must assist the court with prior case law dealing with the issue.

A problem occurs if a computer printout was not generated in the regular course of business, but was printed solely for use in prosecution. If the printout was an accepted business report, but contained data that were entered or transactions that occurred some time significantly prior to the actual printing, an objection may be raised on the grounds "made at or near the time of the act" or "time of preparation."

The problem is compounded in instances where upon securing the computer facility as the crime site, weeks may be needed with the experts to determine what printouts should be obtained. Short of maintaining guards and forbidding use of the computer facility, an option not ordinarily available, the investigator and prosecutor should be prepared to implement extensive, reliable, and provable labeling and identification procedures. Likewise, complete records tracking storage and custody of all evidence items should be maintained. Careful handling of off-line storage devices including computer tapes and disks that may ultimately be used to generate printout evidence is also critical because of their high vulnerability to spoilage or alteration.

A further word of caution is in order. Beware of too much reliance on the testimony of a custodian or other qualified witness to cure single-handedly all foundational problems that the proffered printout is the one generated at the time of the offense or search, especially where the printout constitutes portions of a computer storage printout or other lengthy or complicated computer display. Again, careful and immediate identification of all potential evidence items is necessary.

After all reasonable precautionary steps have been taken to ensure reliability and trustworthiness, the best response to defense business record exception objections is to focus on the law—particularly on the underlying purposes for the law. After the general reliability of the computer system is shown, the court must then be persuaded that within the limitations precipitated by the nature of computer processing, the underlying purposes of the hearsay rule are satisfied.

The issues that have arisen regarding computer records and the law of evidence fall into three basic categories: (1) the admissibility of computer printouts as evidence; (2) computer printouts as the basis of expert testimony; and (3) discovery matters with regard to computer systems. The first category, admissibility, receives the most attention from the courts and commentators. [See, for example: Note, "Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence," 1977 Wash. U.L.Q. 59 (1977); Note, "A Reconsideration of the Admissibility of Computer-Generated Evidence," 126 U. of Pa. L. Rev. 425 (1977).] Each of these categories is discussed below.

a. Admissibility of Computer Printouts as Evidence

The admissibility of computer printouts as evidence depends on whether the data from which the report is generated were captured and entered into the system in the normal course of business. If so, the data record and reports produced subsequently in the regular course of business or even for trial purposes may be admissible. The following types of reports can be produced from data in computer storage media:

Data	Program	Production
Especially prepared	Special	One time
Especially prepared	Utility	One time
Especially prepared	Production	One time
Production	Utility	One time
Production	Utility	Periodic

Data	Program	Production
Production	Special	One time
Production	Production	Periodic

Definitions of the kinds of data and programs given in this tabulation are listed below:

- Especially prepared data: Data are translated from a noncomputer storage medium to computer storage medium.
- Production data: Data are already in the form used for regular and normal production.
- Utility program: A computer program generally available in a computer system and used for different applications. This category includes generalized audit programs.
- Special program: A computer program especially programmed for one specific purpose. It may also call and use utility programs and operating system functions to perform its job.
- Production program: A computer program used in a regularly run production job conducted during normal business activities.

Most decisions regarding the admissibility of computer printouts address the foundational requirements needed to defeat a hearsay objection and show that the computer printouts fit into the business records exception to the hearsay rule. All the decisions surveyed, except one, allowed the admission into evidence of a computer printout. In *Department of Mental Health* vs. *Beill*, 44 Ill. App. 3d 402, 2 Ill. Dec. 655, 357 N.E.2d 875 (1976), the court held that the Department had not met the foundational requirements to introduce the computer-generated records.

Criminal Cases—Courts appear to treat the issue of the admissibility of computer records, both in criminal and civil cases, in a similar manner. In *State* vs. *Watson*, 192 Neb. 44, 218 N.W.2d 904 (1974), a criminal conviction for writing a check with insufficient funds, the defendant objected to the admission of the bank's computer printout that showed the rejected transactions. The court, in addressing the question of sufficient foundation, noted that the Uniform Business Records as Evidence Act required the custodian to testify regarding the identity of the business record, that the record was made in the regular course of business, and that it was made contemporaneously. Then the court must determine whether the sources of information and the method and time of preparation justified admission in light of the broad interpretation that should be given to the Uniform Act.

In *United States* vs. *Weatherspoon*, 581 F.2d 595 (7th Cir. 1978), a conviction for racketeering, mail fraud, and false statements, the defendant enrolled in her beauty school many times the number of VA students allowed. The defendant objected to admission of the government's computer printouts, claiming improper foundation. The court, in rejecting the defendant's claim, held that the printouts were computerized compilations of information from enrollment certification forms that had been submitted by the defendant and simply keyed onto computer tape. Moreover, the testimony of government employees demonstrated the computer system input processes; the accuracy of the printout to 2%; that the computer was tested for internal program errors on a monthly basis; and that the VA made, maintained, and relied on the printouts in the ordinary course of business. Finally, counsel or defendant had been allowed to inquire into the accuracy of the printouts.

Another criminal case, *United States* vs. *Scholle*, 553 F.2d 1109 (8th Cir. 1977) cert. den. 434 U.S. 940, was a narcotics conviction. At trial, the government introduced a computer printout representing a compilation of information regarding cocaine exhibits that were compiled from the regional laboratory of a district office of the Drug Enforcement Administration. The government also presented the testimony of the doctor who developed the computerized compilation system. The compilation revealed that a particular additive to cocaine, which was very uncommon, appeared in only two cases prior to appearing in the cocaine seized and purchased from the defendants. The government was attempting to show, by means of the inference that could be drawn from the compilation evidence, that the defendants were involved in a conspiracy.

In upholding the trial court's exercise of discretion in admitting the compilation, the 8th Circuit noted that the government had provided a proper foundation by demonstrating that the compilations were made routinely and contemporaneously. In addition, the government provided the original source of the computer program and the procedures for input control that ensured accuracy and reliability.

Income tax offense cases often provide situations in which computer records are used as evidence of the tax evasion. In *United States* vs. *Fendley*, 522 F.2d 181 (5th Cir. 1975), the court rejected the defendant's objection to the introduction of computer printouts on the grounds of accuracy. The court noted that similar printouts had been used in criminal proceedings and that computer printouts are not intrinsically unreliable. Finally, the court noted that the defendant had an opportunity to inquire into the processes by which the data were input and retrieved from the system, if he had wished to attack the reliability of the printouts.

In *United States* vs. *Farris*, 517 F.2d 226 (7th Cir. 1975) cert. den. 96 S. Ct. 189, the defendant, convicted of failure to file income tax returns, claimed that the trial court erred in admitting into evidence the output of a computerized data system. The prosecution was not required to show

the accuracy of the records, maintained at the National Computer Center. The defendant also claimed a best evidence rule objection, although the center director certified the authenticity of the printout.

The 7th Circuit upheld the admissions of the records under 28 U.S.C. Sect. 1733(b), which allows admission of authorized copies of documents of United States departments or agencies as if they were originals in order to prove by memorandum an act, transaction, or occurrence. At trial, the printout was offered to show that no record of filing a tax return was found after diligent search, and the lack of that record would be evidence showing that the defendant had not filed a tax return.

Civil Cases—A multitude of different kinds of cases have computer-related evidence issues in the civil arena. In *Sears, Roebuck & Co.* vs. *Merla*, 142 N.J. Super. 205, 361, A.2d 69 (1976), a collection case, the court upheld the admission of a computer printout alone to prove the debt. The printout showed only dates of purchase, cost, departments, credit card number, payments made, and balance due, but could not describe the goods sold. Sears had destroyed the original invoices of the defendant's purchases so that the only evidence available regarding the defendant's account was the printout. The court held that so long as the proper foundation was laid, a computer printout is admissible on the same basis as any other business record.

In another New Jersey case, which was a mortgage foreclosure action, the court delineated the requirements necessary in laying the foundation for business records. In *Monarch Federal Savings & Loan Assn.* vs. *Genser*, 156 N.J. Super. 107, 383 A.2d 475 (1977), the court held that personal knowledge testimony regarding the information received into the computer is not required, nor is it necessary to have the preparer testify. However, the testimony is required of a custodian or other qualified witness who can testify that the computer records were made in the ordinary course of business, that they were made contemporaneously, what the sources of the information were, and the method and circumstances of preparation.

Many states have enacted the Uniform Business Records as Evidence Act. In construing it, most state courts have concluded that computer printouts can be business records. One example is *Missouri Valley Walnut Co.* vs. *Snider*, 569 S.W. 2d 324 (Mo. Ct. of App. 1978), a breach of contract case in which the court held that the computer readouts were admissible under the business records exception to the hearsay rule. Testimony showed that the plaintiff's office manager received information daily from buyers and log inspectors and fed that information into the computer. The computer delivered a printout the following day that was checked for accuracy against the original records.

An interesting twist in this field is the use of computer printouts as summaries prepared specifically for litigation. In *United States* vs. *Smyth*, 556 F.2d 1179 (5th Cir. 1977), a conviction for conspiracy to defraud and defrauding the United States, the defendant objected to the admission of two sets of FBI computer printouts. The defendant complained that the printouts were simply summaries of records made for purposes of the prosecution and that the headings and explanatory keys were prejudicial. The court allowed the printouts to be introduced, but instructed the jury that they were not evidence but only summaries. The court had all of the underlying documents from which the summaries were made in evidence so that, in conjunction with the jury admonition, there were no prejudicial effects from the summaries.

b. Computer Records as the Basis for Expert Testimony

Two 1976 decisions bear on the questions raised when computer records are used as the basis for expert testimony. In *Pearl Brewing Co.* vs. *Joseph Schlitz Brewing Co.*, 415 F. Supp. 1122 (S.D. Tex. 1976), a complex antitrust suit that also concerns the discussion below regarding discovery matters and computer printouts, the defendant requested discovery of the computer information that was the basis of the expert witness's testimony. The issue before the court was whether the product of computer experts and economic experts working together specially to formulate a highly sophisticated and computerized econometric model for the litigation was discoverable as to the detailed structure of the computer model and alternative methods that the plaintiff had considered but rejected.

The computer model was programmed to test a high volume of data, which simulated market conditions. A damage assessment program also was prepared. Notwithstanding that the plaintiffs had been very cooperative in pretrial discovery, had made available to the defendants printouts of both systems, and had offered to make the trial expert available, the defendant claimed that these offers were inadequate and requested the actual detailed structure of the model. The defendant also wanted to take the depositions of those experts who actually developed and tested the systems.

The court held that the detailed structure was discoverable but that the alternative methods were not. It noted that this was not a usual case of business records; rather, the defendant sought expert information prepared specially for trial in a case with exceptional circumstances.

The second case in this same area is *Perma Research and Development* vs. *Singer Co.*, 542 F.2d III (2nd Cir. 1976) cert. den. 429 U.S. 987, 97 S. Ct. 507. The case was a breach of contract suit in which the plaintiffs claimed

breach of the duty to make best efforts. The defendant objected to the use of results of computer simulation as a basis for the plaintiff's expert testimony. The court admitted that the better practice would have been for plaintiffs' counsel to deliver to defense counsel details of the underlying data and theorems used in the simulations before trial so as to avoid discussion of their technical nature during trial. The trial judge was not charged, however, with abuse of discretion for allowing the expert's testimony regarding the results of the computer simulation. The defendant did not show that it had an inadequate basis on which to cross-examine the expert witness.

c. Discovery Matters with Regard to Computer Systems

As was mentioned above, *Pearl Brewing Co.* vs. *Joseph Schlitz Brewing Co.*, 415 F. Supp. 1122 (S.D. Tex. 1976), is one example of the issues raised with regard to discovery and computer systems.

In *United States* vs. *Liebert*, 519 F.2d 542 (3d Cir. 1975) cert. den. 423 U.S. 985, 96 S. Ct. 392, 46 L Ed. 2d 301 (1975), another discovery case, the issue before the court was whether pretrial discovery may be used to secure extrinsic evidence so as to impeach the reliability of a computer printout, a fundamental element of the prosecution's case. The defendant in this case was charged with failure to file income tax returns. The IRS computers had no record of the defendant's filing. The defendant requested that his computer expert have access to the IRS Service Center to analyze and test, particularly for reliability, the IRS data processing system. Such a request was granted. Then the defendant requested, for discovery purposes, records of the notices sent to persons stating that they had filed no returns or none had been received by the IRS.

The court granted the defendant's request for a portion of the list of nonfilers. Because the government refused to comply with the court order, the court dismissed the defendant. On appeal, the dismissal was reversed. The appellate court initially noted that pretrial discovery in criminal cases usually is within the court's discretion. It also noted that the admission of printouts in criminal trials was allowed as long as sufficient foundation was laid showing trustworthiness and allowing the opposing party the opportunity to inquire into the accuracy of the computer and the input process. However, the court held that supplying the list that the defendant requested would be unreasonable because of infringement of the right of privacy of those persons on the list. The court noted that the availability of the lists could lead to the defendant in looking for inaccuracies to contact the persons on the list. The alternative suggestion of the IRS to make available to the defendant all the documents regarding the procedures, operation, and electronic data processing system and the statistical analysis regarding the capability of the IRS to discover nonfilers and allow its expert witness to be deposed was held sufficient to provide the defendant with an opportunity to question the accuracy of the system.

In *United States* vs. *Davey*, 543 F.2d 996 (2d Cir. 1976), also a tax evasion prosecution, the issue before the court was whether the IRS may, by summons, compel a taxpayer to produce computer tape that contains part of its financial recordkeeping system. The trial court held that duplicates of the tape at the expense of the IRS would suffice for purposes of the summons. The Second Circuit Court overruled the trial court stating that the defendant must supply the original tapes at its own expense. This holding was in accord with the revenue ruling that requires companies and computer-based recordkeeping systems to save their tapes.

Finally, *Oppenheimer Fund, Inc.* vs. *Saunders*, — U.S. — 98 S.Ct. 2380, 57 L. Ed. 2d 253, 6 C.L.S.R. 848 (1978), was a class action in which the plaintiffs sought to require the defendant to help in compiling lists so that the plaintiffs could comply with the class action notice requirements. Through depositions of defendant's employees, the plaintiffs determined the class size and discovered that to compile the requested list, someone would have to manually sort through a large volume of paper records, key punch 150,000 to 300,000 computer cards, and create eight new programs at a cost of $16,000.

While the court noted that if the defendant could perform the task with less difficulty and expense than the plaintiff, then the district court could order the defendant to perform it. However, the defendant should not bear the expense. The court rejected the lower court's holding that because the records were kept on computer tapes it was justifiable to impose a greater burden on the defendant. Although the court realized that some defendants may be tempted to use their computer systems to irretrievably bury information and immunize themselves and their business activity from later scrutiny, it rejected that such was the situation in this case.

4. Practical Recommendations

a. Technical Presentations

The most likely image that the judge and jury have of computer technology is what they last read on the front page of the newspaper. This material is sometimes sensationalized and distorted. As with any case, the jury and the judge should thus be left with three or four strong points. The whole case should be made as basic, simple, and free from computer technology and terminology as possible.

In court, only the circumstances and technology necessary to present the case should be explained. It is usually better to rely on paper records when they exist rather than to introduce computer-generated records.

The "bits and bytes" of computer logic should not be presented when decimal numbers, letters of the alphabet, and phenomena external to the computer will suffice. Juries do not have to understand telephony to convict an obscene telephone caller. When a case involves computer programs, the source language forms should be used and compilers, assemblers, and object language forms should be ignored when not essential to the case. Whenever possible, using analogies to familiar objects is useful in presenting technical concepts; some examples are provided below:

Computer-Related	Analogy
Magnetic tape and tape drives	Cassette and reel-to-reel, audio recordings, and hi-fi equipment
Magnetic disk	Phonograph record
Optical disk	Compact disk (CD)
Computer printer and output listing	Printing adding machine, typewriter
Computer terminal with printer	Typewriter
Computer terminal with display	Cable television and home TV games
Computer programs	Food recipes, player piano rolls
Addressable storage	Post office boxes
Terminal access passwords	Combination locks
Data communication	Telegrams or telex
Real-time and nonreal-time	Selecting food in a cafeteria and ordering from a waiter
Batch and on-line	Using a home dishwasher and using a continuous flow dishwasher in a restaurant
One microsecond (one millionth, 0.000001) compared to one minute	One minute compared to 114 years

As stated earlier, avoiding computer field jargon such as software (computer programs), firmware (computer programs in read-only storage devices), bits (binary digits), IBM cards (punch cards), and bugs (computer program errors) is important, as is using the most technically correct, dictionary-defined words and maintaining strict differentiation between living persons and computers. Computers are not dumb or smart and do not make errors or commit crimes; only people have these attributes. Errors that result from computer actions stem from human actions such as input errors (garbage in, garbage out), electronic design errors, lack of proper maintenance, or program errors.

Computers should not be personified in courtroom presentations. Computers should be treated strictly as inanimate objects, machines, subject to use and manipulation by people. When the judge and jury need an explanation to understand technical issues, simple diagrams and visual aids should be used extensively.

Visual aids can be used effectively in computer crime cases and are often readily available or easily prepared. Many of the diagrams and tables in this manual may be useful. The following visual aids are suggested:

Visual Aid	Use
Programmable pocket calculators	Computer program concepts
Pocket calculators	Illustration of input, output, storage, and number representation
Computer terminal installed in the courtrooms with access to a time-sharing service [optional closed circuit television (CCTV) for more effective viewing of terminal]	Demonstration of all computer time-sharing concepts and computer applications
Charts	Data flow, programming concepts, computer concepts
Photo blowups	Evidence detail, computer equipment detail
Tapes, disks, diskettes	Examples of computer media
Computer vendor-provided motion picture films	Presentation of most computer concepts

When large volumes of writing are to be presented in court, the best evidence rule may be inapplicable. Therefore, California prosecutors should refer to code number 1509 of the California Evidence Code regarding "compilation evidence." One time-saving recommendation for cases with a large volume of evidence is to assemble a single exhibit book containing all documents, send copies to the defense and to the judge, and introduce it as a single exhibit in court. A record of exhibits, the counts each is connected with, and the names of the witnesses who are to testify about each item should also be prepared.

b. Immunity

Some kind of immunity is necessary in complicated computer cases. Coconspirators are needed as witnesses because the problems of proof are difficult without them. If they are granted immunity, however, the jurors tend to be lenient with the defendant; for that reason, some prosecutors try to avoid formal immunity. A prosecutor could tell the suspects that they are likely to be prosecuted, yet indicate that their testimony would be a mitigating factor. Another point is that juries usually do not sympathize with the victim that is a large business or government agency that could "afford the loss."

c. Judges

Judges vary widely in their knowledge of computer technology and in their attitudes concerning the knowledge they think they have of computer technology. On the basis that a little knowledge can be a dangerous thing, a judge who has had a brief course on computer technology may be more difficult to deal with than a judge who has had no instruction in computer technology. Brief courses on computer technology make the technology too simple in too many respects. The effort required to develop computer programs, the likelihood of adequate integrity of computer programs, and the complexity of the programs can often be made deceivingly simple.

SECTION VI: Computer Crime Law

This section is designed to aid investigators and prosecutors by summarizing state and federal statutes applicable to computer crime. It covers them in the following order: state penal laws, secondary state penal laws, federal penal laws, secondary federal penal laws. Some portions of this section have not been updated since 1979 but are still valid and useful. In 1979 prosecutors stated that existing statutes could be found to prosecute all cases of computer crime coming to their attention. The laws were not written in anticipation of high technology crime, however, and in some cases prosecution was difficult and obtuse.

In the intervening decade, the need for laws directly applicable to computer crime became even more apparent, and most states now have computer crime statutes. Two federal statutes, the Computer Fraud and Abuse Act (PL 99-474) and the Electronic Communications Privacy Act (PL99-508) were enacted in 1986. The rapid rate at which new laws are being adopted makes it difficult for any discussion to be completely timely. The material in this section added since the first edition is based in part on a 1985 study of prosecutorial experience with computer crime performed for the U.S. Department of Justice, Bureau of Justice Statistics[10], and on other research[35]. A broad range of state and federal laws are discussed in addition to computer crime statutes.

A. State Penal Laws

1. Legislative Response to Computer Crime

Appendix B cites the states that have enacted computer crime laws. These laws vary widely in offense named, definitions, and sanctions. This disparity stems from a number of causes, including:

- Response to local concerns
- Desire to correct specific shortcomings of existing law
- Apparent lack of understanding of the crimes and associated technology
- Interest in adopting computer crime laws similar to those passed earlier in other states
- Need to accommodate the new law to an existing statutory scheme.

Computer crime has been broadly defined as any illegal act that requires the knowledge of computer technology for its perpetration, investigation, or prosecution. Computer crime is not a single type of crime; rather, most nonviolent crimes and even violent crimes such as homicide can be committed through or facilitated by computers.

Crimes directed at computers and information media can also include violent physical attacks as well as technical manipulations. New definitions applicable to specific actions have now been included in each of the state computer crime statutes and the federal computer crime laws.

State computer crime statutes fall into four general categories:

- *Property expansion*. Expansion of the definition of property in existing state criminal statutes to include computer systems, computer programs, data, and computer services.
- *Focused scope*. A new statute with a specific focus on a particular type of crime such as debit card fraud.
- *Broad scope*. A new statute with a broad focus to address fraud perpetrated by computer manipulation as well as damage to computer hardware, systems, programs, and data stored in computer systems.
- *Extended scope*. A new statute with a broad scope, with additional coverage for denial of use of a computer system, damage or theft to computer programs, or trespass into computer systems.

The computer crime offenses covered by these statutes are further detailed below using examples of definitions from state statutes.

a. Computer Fraud

In Arizona computer fraud is committed by:

> . . .accessing, altering, damaging or destroying without authorization any computer . . . with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises.

Generally, the computer fraud provisions of other states resemble the Arizona model. Furthermore, they usually apply to accessing any aspect of the computer system.

b. Computer Trespass or Computer Tampering

Under the computer trespass provision found in at least 22 states, a crime is committed if a person accesses a computer without authorization. This definition covers intrusion into computers by perpetrators (including hackers) through telephone circuits. Many of these provisions are similar to the Georgia statute that includes access in its enumerated activities constituting computer tampering: "Any person who intentionally and without authorization,

directly or indirectly accesses, alters, damages, destroys... any computer... shall be fined... or imprisoned." In addition, the Florida law proscribes trespass in two contexts, separately stated: (1) offenses against intellectual property; and (2) offenses against computer equipment or supplies.

c. Credit Information Tampering

Some state statutes specifically proscribe computer tampering in order to obtain unauthorized credit information from a computer or to introduce false information into a computer. The Hawaii statute, for example, provides that an individual has committed a crime if:

> ...[h]e accesses or causes to be accessed any computer, computer system, computer network, or any of its parts with the intent to obtain unauthorized information concerning the credit information of another person or who introduces or causes to be introduced false information into that system or network with the intent to wrongfully damage or enhance the credit rating of any person.

d. Trade Secret Tampering

California, Florida, Massachusetts, Nevada, and Wyoming have computer crime statutes that forbid the taking of trade secrets. The provisions are very different in nature but similar in effect. The California and Massachusetts statutes are broad, addressing the wrongful taking of a trade secret in many contexts including those stored in computers. The California law expressly proscribes stealing, taking, carrying away, or using, fraudulent appropriation, and unlawful or lawful access followed by a wrongful copying of the trade secret.

e. Disruption of Computer Services

Another computer offense proscribed in several statutes involves the disruption (or, in some states, degradation) of computer services. The Missouri statute provides that "a person commits the crime of tampering with computer users if he knowingly and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services..."

2. Technical Definitions in State Computer Crime Laws

The technical definitions in the state laws also vary. Many states have followed the definitions proposed in early federal bills.* These definitions have been heavily criticized by the technical community in Congressional hearings as ranging from being too dependent on current technology to being inaccurate or irrelevant. However, they prevailed and are found in the Computer Fraud and Abuse Act of 1986.

*Senate Bill 1766, the Federal Computer Systems Protection Act of 1977.

Vestiges of the terminology used in the early federal bills appear in several state statutes. For example, the term "access," a key term in most computer crime statutes, is most often defined as "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer." It is so defined in about a third of the states.

The use of the word "approach" in the definition of "access," if taken literally, could mean that any unauthorized physical proximity to a computer could constitute a crime. It also may derive from preexisting definitions of access in trade secret theft statutes.

Most of the statutes define "computer," although approaches to the definition vary. The most prevalent definition is that a computer is an electronic device that performs certain functions: logic, arithmetic, or memory. In addition, the prevailing definition attempts to include data, software, and communications facilities connected or related to the electronic device in a system or network. This definition could theoretically include an entire public telephone system as part of a computer that has dial-up telephone access.

Concern that the definitions are too broad and could include anything from a digital watch to the entire telephone system resulted in various exclusions. In one state exclusions are a radio or television transmitter or receiver, television camera, video tape recorder, sound recorder, phonograph, or similar device used for reproducing information in aural or visual form without changing the nature or content of the information, unless such a device is connected to and used by a computer. California excludes automated typewriters or typesetters, portable calculators, or computers used for personal, family, or household use and not used to access other computers without any further clarification as to meaning.

These varying definitions demonstrate the confusion resulting from a complex, rapidly changing technology. For example, "automated typewriter" is not a term in general use, and its meaning is ambiguous and changing as technology advances. It could be an electric typewriter, a typewriter under computer control and without a keyboard or storage buffer, a "self-erasing" typewriter, a "dumb" (without local processing capabilities) or "smart" (with such capabilities) computer terminal, a word processor, or in the future a voice-activated data input device.

Some states use as the definition of "computer" an internally programmed device that processes data. Others limit the programmed device to a general-purpose digital device. One uses the same approach with the word "programmable" instead of "programmed," which may raise a problem if a dedicated-use device, such as an automated teller machine, is used in a suspected criminal act. Further, the

defined functions of computers sometimes redundantly include storage as well as logic, arithmetic, and memory. A few states and the U.S. Congress in the federal computer crime laws, apparently contemplating technological developments beyond the electronic, expand the adjectives applicable to the device that may be considered a computer, including magnetic, optical, electrochemical, or other high-speed data processing device or system.

"Computer network" has many definitions in state statutes. Some define "computer network" as "the interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more interconnected computers." One state expressly includes microwave or other electronic communication means for interconnecting computers. Another commonly followed definition of "computer network" is as follows:

> A set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

One state shortens the definition to "an interconnection of two or more computer systems." Some states use the term "computer program," others use the term "computer software," and some use both even though the meaning of the two often overlaps. Nearly half of the states with computer crime statutes use the term "computer software" and define it as "a set of computer programs, procedures and associated documentation concerned with the operation of a computer system." "Computer software" is one of the few terms to be consistently defined in all states that use the term in their computer crime statutes. Unfortunately, "software" as used in computer technology parlance is jargon that has many significantly different definitions.

Another term that has presented definitional difficulties is "data." Only two states use precisely the same language. In every other state, some minor differences appear. One defines "data" simply as information of any kind in any form including computer software. Two others classify data as intellectual property.

In the definition of "financial instrument," the following terms appear in the various state statutes: check, cashier's check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, marketable security, warrant, note, negotiable instrument, transaction authorization mechanism, and any computer system representation thereof. Most of the items appear in almost all state statutes.

"Property" is still another term that is defined slightly differently in all states. One typical state statute definition of property seems to include most, if not all, of the elements used in different form:

> Any tangible or intangible item of value that includes, but is not limited to, financial instruments, geophysical data or the interpretation of that data, information, computer software, computer programs and computer-produced or stored data, supporting documentation, computer software in either machine or human readable form and any other tangible or intangible item of value.

Another state defines "property" simply as "anything of value" and then lists numerous examples, including "computer programs or data."

These examples illustrate the inconsistencies, inaccuracies, and limitations in the definitions of important terms used in the computer crime statutes of different states. In a few years voice data entry and output, digitized voice, knowledge-based systems, lasers, optics, molecular-based logic, and neural logic could result in new methods and evidence of crime for which current laws might be inadequate.

There are now as many different and conflicting definitions of computer crime as there are states with computer crime statutes. The definitions of those terms, their comprehensibility, rate of obsolescence, and ease of application will play an important role in determining how successfully and effectively these new statutes will be used to deter and prosecute computer crime.

3. Penalties in State Computer Crime Laws

State legislatures have taken a variety of approaches to providing punishment for computer crime. Generally, the computer crime statute itself does not explicitly state the fine or term of imprisonment to be prescribed to a convicted person. Instead, the penalty provisions classify the computer crime as a particular felony or misdemeanor. To determine the scope of the penalty, one must refer to the general criminal penalty statute of that state. Delaware's computer crime statute illustrates this point. It simply provides that "computer fraud is a class C felony and computer misuse is a class E felony." Even more simply, Idaho prescribes a general felony penalty for computer fraud and computer tampering and a misdemeanor penalty for unlawful computer access.

A few computer crime statutes expressly delineate the bounds of the penalties. For instance, the Oklahoma statute sets forth a fine of $5,000 to $10,000 and/or confinement in the state penitentiary for 1 to 10 years for conviction of a felony under the computer crime law. Rhode Island's penalty section provides for a fine of not more than $5,000 and/or imprisonment for not more than 5 years for commission of a computer crime.

4. Prosecutorial Experience with State Computer Crime Laws

Prosecutors interviewed for the 1985 study reported a number of experiences:

- Only a few of the many incidents investigated resulted in prosecution, primarily because the evidence available did not appear to support indictment. Some prosecutors reported that grand juries failed to understand the case because of the technical nature of the acts involved.
- More perpetrators now seem to be mounting a defense than did those prosecuted in the past. The most actively defended recent cases have been those involving electronic trespass.
- Many prosecutors interviewed were unaware that their state had a computer crime law.
- Some prosecutors reported that because penalties for violation of their computer crime laws are less than under those for traditional theft and burglary laws, they favor use of the more stringent statutes.
- Many prosecutors chose to use the computer crime law only when a traditional fraud, theft, or malicious mischief statute was clearly less applicable.

Prosecutors expressed concern about a number of legal issues related to specific statutes in their state:

- Existing traditional law is not applicable to fraud or larceny by trick when the deceived party is a device (e.g., automated teller machine, vending machine, turnstile, computer). The computer crime statute enacted to address that issue is now considered to be too narrow in focus.
- The definition of "access" taken from the language of an early federal bill that has been adopted by 22 states is too vague. It includes the word "approach," which is appropriate for physical action but not electronic action.
- A recent amendment to the California computer crime law makes electronic trespass without malice a crime and thereby addresses a loophole in many statutes; however, it exempts from the statute such trespass by employees.
- Prosecutors in several states reported a preference for using traditional theft statutes when possible because of their known interpretation by the courts and stronger penalties available.
- One state statute requires victims to report incidents of computer crime to the public authorities. Prosecutors reported that this provision may be unconstitutional.

5. Timeliness of the Law

The focus of computer crime legislation has been on the current technical aspects of criminal methods and the current technical development of computer products rather than on the more germane but difficult subject of offenses against the information assets at risk, independent of the technology used. The result has been laws that can become quickly obsolete as the technology and its applications change and new technical methods of engaging in information-related crime appear. For example, juvenile hacker attacks on computers demonstrated the absence of laws dealing with electronic criminal trespass into computers. An additional symptom may be the difficulty of producing adequate technical definitions for computer crime laws.

Prosecutors are inhibited from using computer crime laws by their and the court's lack of computer literacy and the availability of older laws more familiar to them, even though those laws may not be the best or most applicable. Prosecutors report that failure of victims to report suspected computer crimes and to cooperate with prosecution discourages them from developing the capabilities necessary to work in this area of the law. Data communications advances, moreover, have transcended jurisdictional boundaries, causing criminal acts and their effects to fall into different jurisdictions. The concept of geographical proximity is being replaced with electronic proximity as computers become connected to communication circuits. In addition, the perpetration of crimes at remote computer terminals with only electronically produced means of identification of suspects and recording of their activities makes obtaining adequate evidence difficult.

6. Computer Crime Laws of Selected States

Appendix A contains the text of representative state statutes; citations of computer crime statutes are presented in Appendix B. Five state laws are summarized and briefly analyzed below.

a. Florida Computer Crime Act

Summary—The Florida Computer Crime Act [Fla. Stat. Ann. Sect. 815.01 et seq. (West Supp. 1979)] proscribes several offenses against intellectual property including data and programs, offenses against computer equipment and supplies, and offenses against computer users. Intellectual property includes programs and data existing within or without a computer (system or network). The offenses against intellectual property are willfully and without authority: (1) modifying data, programs or supporting documentation; (2) destroying data, programs, or supporting documentation; and (3) disclosing or taking data, programs, or supporting documentation that are trade secrets or confidential. Such acts are felonies of the third degree

unless the offense is committed for the purpose of devising or executing a scheme or artifice to defraud or obtain any property, in which case the crime is a felony in the second degree.

Offenses to computer equipment and supplies (the terms are not further defined by the law) include willfully, knowingly, and without authorization modifying such equipment or supplies. That crime is a misdemeanor of the first degree unless the offense is for the purpose of devising a scheme or artifice to defraud or to obtain any property, in which case the offense is a felony of the third degree. The offense of willfully, knowingly, and without authorization destroying, taking, injuring, or damaging a computer (system, network) or equipment or supplies used or intended to be used in a computer (system, network) is a misdemeanor of the first degree if the damage is $200 or less and a felony of the third degree if the damage is between $200 and $1,000. If the damage is $1,000 or more or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, the felony is of the second degree.

Offenses to computer users include willfully, knowingly, and without authorization accessing or causing to be accessed a computer (system, network) or willfully, knowingly, and without authorization causing the denial of computer system services to an authorized user of the services which are owned by, under contract to, or operated for, on behalf of in whole or in part, or in connection with another. The offense is a felony of the third degree unless it is committed for the purpose of devising or executing a scheme or artifice to defraud or obtain property. In that event the offense is a felony of the second degree.

Finally, the law states that it is not intended to preclude the applicability of other Florida criminal law.

Analysis—The law covers acts or theft of and damage to computer equipment, supplies, programs, and data. It covers willful, unauthorized access to computers (systems, networks) and denial of services to users. The offenses to intellectual property (programs and data) apply whether or not the property is stored inside a computer: that is, the law applies to programs and data contained in listings, tapes, disks, cards, and other off-line and on-line media of expression. The law does not require the media of storage to be a "thing," and consequently, electronic impulses should be includable. Such inclusion will ease the finding of a taking when a program is taken, modified, or destroyed over telephone lines, as in the *Ward* [Ward 1972] and *Seidlitz* [Seidlitz 1978] cases.

Because "unauthorized" is not defined by the law and because "access" is defined so poorly, the prohibition against theft of computer services such as computer time is not clearcut. Florida appears to have no specific theft of services statute, and the property theft statute [Fla. Stat. Ann. Sect. 811.021(1)(a) (Supp. 1975)], "anything of value," would have to be interpreted to include services. Because applicability of both the new law and the prior property theft law is unclear, obtaining a conviction for theft of services such as computer time may remain difficult in Florida.

A particular advantage of the Florida law is that computer programs or data stored other than in a computer qualify as intellectual property within the meaning of the statute. This fact will aid in the prosecution of thefts, disclosures, alterations, and destructions that do occur to computer products but were not covered by prior law.

b. Colorado Computer Crime Law

Summary—The Colorado Computer Crime Law [C.R.S. Sect. 18-5.5-101(1973, 1978 Repl. Vol.)] proscribes the knowing use of a computer for fraudulent purposes, the assault or malicious destruction of a computer, and the unauthorized use of alteration of a computer or its "software" or data. Penalties relate to the value of the item stolen: under $200 of loss or damage is a misdemeanor punishable by a fine and jail sentence up to 12 months; loss or damage over $200 is a felony punishable by a fine and jail sentence up to 40 years.

Offenses that are fraud-related are those in which knowing use ("use" is defined to mean to instruct, communicate with, store data in, retrieve data from, or otherwise make use of a computer, computer system, or computer network) is made of a computer (system, network) for the purpose of devising or executing a scheme to defraud; obtaining money, property, or services by false pretenses; or committing theft.

The other form of computer crime is the knowing and unauthorized use, alteration, damage, or destruction of a computer (system, network).

The graduated classification of offense and associated penalties relate to the dollar value of the loss. Currently, these are: under $50 is a Class 3 misdemeanor, $50 to $199 is a Class 2 misdemeanor, $200-$9,999 is a Class 4 felony, and $10,000 and above is a Class 3 felony. (The Class 3 felony also includes offenses, such as child abuse, that result in serious bodily injury.)

Analysis—This legislation is modeled on the Florida law; however, it is narrower in coverage in that data and programs must be "contained in such computer . . ." to be the subject of the Colorado law damage, alteration, or destruction provisions. It also appears that theft or fraud involving property (which includes information and electronically produced data and "software") must be accomplished by use of a computer to fall within the prescriptions of the law.

Further, there is no sanction for denial of computer services unless such denial is part of a scheme to defraud.

The law is in response to the inadequacies of existing law in that it did not contemplate computer abuse and could not be stretched to accommodate the new forms of wrongful activity. In particular, in a case decided by the Colorado Supreme Court sitting *en banc* on March 19, 1979, the court held that the unauthorized reading and later transcription of a medical record without a taking of the physical record did not constitute a theft because the medical information was not a "thing of value" within the meaning of the theft statute. (*People* vs. *Home Insurance Co.*, No. 27984.)

The law's definitions—the weak point in most existing and pending computer crime legislation—are somewhat more precise than other attempts in this area, but there are still problems with defining "software" and "hardware" in the dynamic technological milieu.

c. Arizona Computer Fraud

Summary—The Arizona statute [Ariz. Rev. Stat. Ann. Sect. 13-2301 and Sect. 13-2316 (Swest 1978)] in its general criminal fraud provisions defines in Sect. 13-2301 for the purposes of Sect. 13-2316 various terms with regard to computers—e.g., "access, computer, computer network, computer program, computer software, computer system, financial instrument, property, and services." Section 2316 provides for the offense of computer fraud. This section states that a person commits computer fraud by accessing, altering, damaging, or destroying without authorization any computer, computer system, computer network with the intent to devise or execute any scheme or artifice to defraud, deceive,or control property or services by means of false or fraudulent pretenses, representations, or promises.

Computer fraud in the first degree, punishable by up to 5 years in prison, is committed when a person accesses, alters, damages, or destroys a computer (system, network) without authorization and with intent to devise or execute a scheme to defraud or to control property or services by false or fraudulent pretenses.

Computer fraud in the second degree, punishable by up to 1-1/2 years in prison, is committed by an "unauthorized intentional access, alteration, damage, or destruction of a computer (system, network) or any software, program, or data contained therein."

Analysis—This law, which was passed at about the same time as the Florida law but independent thereof, is similar in that it covers hardware, programs, and services. Note that "software, programs, and data" must be contained in the computer before such "data and programs" are covered by the law. Otherwise, other Arizona law applied to intellectual or intangible property will have to be applied. The legislature has coined a definition of "software" that encompasses a related group of programs, procedures, and documentation associated with the operation of a computer system. It is of utmost importance when applying any computer crime law to read carefully the definitions therein because they will differ from each other and unfortunately from common usage in the computer field as well.

d. California Basic Computer Crime Statute

Summary—The California Computer Crime Statute [Calif. Rev. Stat. 1987, Sect. 502, Ch. 1499 (1 January 1988)] has been modified three times in response to advances in technology and computer crime methods and offenses. It covers five offenses: (1) manipulating data, a computer system, or computer network to devise or execute a fraud; (2) knowingly accessing and without permission taking copies or using any data from a computer or taking any supporting documentation, internal or external, to a computer; (3) theft of computer services; (4) knowingly accessing and without permission damaging data, computer software, or computer programs, internal or external, to a computer; and (5) disrupting or denying computer services to an authorized user. The last two offenses cover electronic trespass into a computer, computer system, or computer network.

An infraction of the last two offenses is punishable by a fine not exceeding $250. However, if the victim's expenditure exceeds $5,000, the penalty is a fine not exceeding $5,000 or 1 year in prison. Penalties for the other three offenses are a maximum of $10,000 and up to 3 years in prison. Civil action for compensatory damages is provided. Multiple jurisdictions in which offenses occur are allowed to result in criminal or civil action in any of the jurisdictions.

Computer or computer-related materials may be seized under warrant or arrest and forfeited. (Forfeiture of seized property is pursuant to Section 502.01, which is an error in the statute since the code has no such section.)

Exempted from prosecution is any employee accessing the employer's computer system when acting outside the scope of lawful employment so long as the employee's activities do not cause an injury exceeding $100. The conduct of minors is imputed to the parent or legal guardian.

Analysis—The most recent additions to this law cover the offense of electronic trespass, identification of the victim's expenditure, and provision for confiscation of seized equipment and materials. The losses incurred are identified as the victim's expenditures rather than direct or absolute losses. The victim's expenditures include the efforts necessary to verify that anything was or was not altered, deleted, damaged, or destroyed because of the suspect's access to the victim's computer or computer network. These new provisions are quite innovative and may form the basis of a model for updates to other state laws.

The trespass provision covers hacker intrusion attacks where no other offense may occur other than browsing among data files. This provision is more liberal than the New York State statute that requires due notice be given to a potential intruder in a display screen warning. However, other California statutes may require this warning.

The exemption of employees from prosecution is meant to protect whistle blowers, but it presents a difficult challenge for the prosecutor who must produce strong evidence that the suspected employee did not know that his or her act was not authorized. If the prosecutor cannot prove that the act was not authorized, no offense has occurred. The $100 damage limit by an employee does not specify the period the loss occurs and does not include compensation for the victim's expenditures as part of the penalty.

The technical definitions are similar to those in other state laws. Computer network is more simply defined, however, to mean two or more computer systems connected by telecommunication facilities. Computer program is equivalent to software. The definition of computer system excludes nonprogrammable calculators capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data. This definition will become obsolete rather quickly as calculators increase in capability.

Data may be in any form—in storage media, in transit, or presented on a display device. This definition is an important extension of those in other state statutes because data are in transit for significant periods. Because of the broad definitions of these technical terms, offenses can include acts against data and computer programs in the vicinity of computers.

e. New York Offenses Involving Computers [NY Book 39, Sect. 156]*

Summary—New York has several new penal laws designed to meet the problems of computer crime:

- Creation of the new crimes of unauthorized use of a computer [Sect.156.05] and computer trespass [Sect.156.10] designed to deal with the unauthorized use of a "computer" or "computer service."
- Creation of the new crimes of computer tampering in the first degree [Sect.156.25] and in the second degree [Sect.156.20] to deal with the unauthorized and intentional alteration or destruction of a "computer program" or "computer data."
- Creation of the new crimes of unlawful duplication of computer-related material [Sect.156.30] and criminal possession of computer-related material [Sect.156.35], the former designed to deal with the unauthorized duplication of a "computer program" or "computer data," and the latter designed to cover the unauthorized possession of such duplicated material.
- Creation of a new subdivision of the crime of theft of services [Sect.165.15(10)] to make it a crime for a person who, with intent to avoid payment for the use of a "computer" or "computer service," avoids paying the lawful charge. Further, the term "computer service" is included in the definition of the term "service" as that term is defined for the article involving theft [Sect.155.00(8)], and would thus include certain thefts of a computer service in such existing crimes as theft of services by a stolen credit card [Sect.165.15(1)] and unlawful use of credit card [Sect.165.17].
- Application of the existing crimes of larceny, forgery, false written instruments, and related offenses to such conduct as it relates to a computer program or computer data by inclusion of the terms "computer data" and "computer program" within the definition of the following terms:
  - "Property" as defined for the title involving theft [Sect. 155.00(1)]
  - "Written instrument" as defined for the article involving forgery and related offenses [Sect. 170.00(1)]
  - "Business record" and "written instrument" as defined for offenses involving false written instruments [Sects. 175.00(2)and (3)].

To ease the sometimes elusive venue of an electronic medium crime, an amendment to the Criminal Procedure Law (20.60) has provided that: "A person who causes by any means the use of a computer or computer service in one jurisdiction from another jurisdiction is deemed to have personally used the computer or computer service in each jurisdiction."

Analysis—The terms "computer," "program," and "data" may have a commonly understood usage. Unlike the generally understood definition of "computer," however, Sect. 156.00 defines it to include various peripherals designed to store, retrieve, or communicate the results of computer operations, programs, or data. The term "computer service" appears to have been devised to refer to the ever-expanding telecommunication industry that supplies information and services via computers (e.g., Westlaw).

The term "computer material" is a list of certain kinds of computer programs and data. The purpose of the term is to single out the listed programs and data for felony treatment when such programs and data are either invaded

* Much of the text in this subsection was written by William C. Donnino in the commentary to the law.

without authorization [Sect. 156.10(2)] or are altered or destroyed [Sect. 156.20(3)].

A common element of both unauthorized use of a computer and computer trespass is the defined term "uses a computer or computer service without authorization" [defined in Sect. 156.00(6)]. Critically, that term requires *both* that the user lack authorization to use the computer or computer service *and* that actual or specified forms of constructive notice to that effect be given to the user. Proof of constructive notice by showing that the computer was programmed to automatically provide such notice is "presumptive evidence," a permissive inference, that such notice was given.

Effective and provable notice of the lack of authorization to use a computer is further highlighted by the available defense that "the defendant had reasonable grounds to believe that he had authorization to use the computer" [Sect. 156.50(1)]. "Reasonable grounds" imports an objective element in the determination of whether the defendant's belief that he had authorization to use the computer would be one a reasonable person, in the defendant's situation and circumstances, would have. [Cf. *People* vs. *Goetz*, 68 N.Y.2d 96 (July 8, 1986).] Noticeably absent as an available defense to the defendant who may have had authorization to use the computer but not a computer service is the claim that the defendant had reasonable grounds to believe that he had authorization to use the computer service.

The second element of the unauthorized use of a computer is proof that the computer had a device or coding system designed to prevent the unauthorized use of the computer or computer service.

The threshold requirements of notice and a system to prevent unauthorized use in order to be held criminally liable for the crime of "unauthorized use of a computer" were deliberately incorporated into the law in order to encourage greater self-protection on the part of the computer industry.

For the computer trespass crime, however, a system need not prevent unauthorized use. Computer trespass requires the notice, and the neither knowingly gaining access to "computer material," defined in Sect. 155.00(5) to mean certain kinds of programs or data listed in the definition, or "an intent to commit or attempt to commit or further the commission of any felony."

No felony need be committed; at a minimum it need only be intended; and the circumstances surrounding the use of the computer or computer service may supply the inference of the requisite intent. [Cf. *People* vs. *Mackey*, 1980, 49 N.Y.2d 274, 425 N.Y.S.2d 288, 401 N.E.2d 398.]

Since the crime of unauthorized use of a computer contains an element not contained in the computer trespass crime, it is not a lesser included offense of the computer trespass crime. [See *People* vs. *Glover*, 1982, 57 N.Y.2d 61, 453 N.Y.S.2d 660, 439 N.E.2d 376.]

The basic crime, computer tampering in the second degree, requires that a person use a "computer" [defined in Sect. 156.00(1)] or a "computer service" [defined in Sect. 156.00(4)] and without the right to alter or destroy a computer program or data, he intentionally does so. First, a computer or computer service must be the instrumentality of the crime. The unauthorized and intentional destruction of a disk containing a program or data may be criminal mischief, but it is not computer tampering. Second, in addition to showing that the defendant had no right to alter or destroy the program or data, it may be necessary to negate the defense that the "defendant had reasonable grounds to believe that he had the right to alter in any manner or destroy the computer data or the computer program" [Sect. 156.50]. "Reasonable grounds" imports an objective element in the determination of whether the defendant's belief that he had authorization to use the computer would be one a reasonable person, in defendant's situation and circumstances, would have. [Cf. *People* vs. *Goetz*, 68 N.Y.2d 96, (July 8, 1986).] Third, the consummated crime requires the actual alteration or destruction of a program or data.

Computer tampering in the first degree initially requires commission of computer tampering in the second degree. Thus, the later crime is a lesser included offense of the former. [See *People* vs. *Glover*, 1982, 57 N.Y.2d 61, 453 N.Y.S.2d 660, 439 N.E.2d 376.] The second requirement of the crime is the commission of one of four aggravating elements. The first alternative is that the defendant acted with the intent to commit or attempt to commit or further the commission of a felony. No felony need be committed; at a minimum it need only be intended; and the circumstances surrounding the use of the computer or computer service and the material destroyed may supply the inference of the requisite intent. [Cf. *People* vs. *Mackey*, 1980, 49 N.Y.2d 274, 425N.Y.S.2d 288, 401 N.E.2d 398.]

The second alternative is that the defendant had previously been convicted of a computer offense that is defined in Article 156, or theft of services of a computer or computer service defined in Sect. 165.15(10). Curiously, albeit the law creating these new crimes also expanded the crimes of larceny, forgery, false written instruments, and related offenses to include such conduct as it relates to a computer program or data, a prior conviction of those crimes is not an authorized predicate for the commission of computer tampering in the first degree.

The third alternative is that the computer program or data altered or destroyed be those specifically listed as "computer material" in Sect. 156.00(5). The fourth alternative

is that the program or data be altered or destroyed in an amount exceeding $1,000, a sum that parallels the distinction between misdemeanor and felony crimes defined by the value of the property involved.

The new crime of unlawful duplication of computer-related material [Sect. 156.30] is designed to deal with the unauthorized duplication of a "computer program" [defined in Sect. 156.00(1)] or "computer data" [defined in Sect. 156.00(3)]. A related new crime is criminal possession of computer-related material [Sect. 156.35], which is designed to prohibit the unauthorized possession of a program or data duplicated in violation of the crime of unlawful duplication of computer-related material, and possessed with intent to benefit the possessor or a person other than the owner.

The theft of a program or data, through unauthorized duplication, is a crime peculiar to the electronic media. Unlike a traditional larceny, valued and valuable programs or data can be taken without disturbing the rightful owner's possession and without depriving the rightful owner of the program or data. Nevertheless, the program or data can be appropriated by duplication in seconds.

The crime of unlawful duplication of computer-related material requires more than unauthorized duplication. It requires an economic deprivation in excess of $2,500, or irrespective of the amount of economic deprivation, an "intent to commit or attempt to commit or further the commission of any felony." Absent the criminal purpose and absent an economic deprivation of $2,500, the unauthorized duplication of a program or data is not violative of Sect. 156.30.

As with the other computer crimes that make a criminal purpose an aggravating element of the offense, no felony need be committed; at a minimum it need only be intended; and the nature of the program or data duplicated and the circumstances surrounding the duplication may supply the inference of the requisite intent. [Cf. *People* vs. *Mackey*, 1980, 49 N.Y.2d 274, 425 N.Y.S.2d 288, 401 N.E.2d 398.]

Finally, in addition to showing that the defendant had no right to duplicate the program or data, it may be necessary to negate the defense that the "defendant had reasonable grounds to believe that he had the right to copy, reproduce, or duplicate in any manner the computer data or the computer program." [Sect. 156.50(3).] "Reasonable grounds" imports an objective element in the determination of whether the defendant's belief that he had authorization to duplicate the program or data would be one a reasonable person, in the defendant's situation and circumstances, would have. [Cf. *People* vs. *Goetz*, 68 N.Y.2d 96, (July 8, 1986).]

B. Other State Authority Bearing on Computer Crime

1. Automatic Banking Device

Kentucky has a statute [Ky. Rev. Stat. Sect. 434. 685 (Supp. 1978)] that proscribes the misuse of electrical information with regard to automatic banking devices and electronic fund transfers (EFTs). A federal law, Title XX of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), also proscribes EFT crimes.

2. Credit Card Crime

Many computer crimes consist of or include unauthorized access of a computer system to obtain, alter, damage, or destroy programs, data, or services, such as computer usage. Apart from theft of computer programs (which is discussed separately below), it may be possible to charge a perpetrator with credit card crime, forgery, theft of property, services, or a thing of value under charges of false pretenses and burglary[36]. Most jurisdictions have credit card abuse laws. For example:

- AL Code Tit. 13 Sect. 4-32 4-41 (1977)
- AK Stat. Sect. 11.46 2285 (fraudulent use of credit card), Sect. 11.46.290 (obtaining a credit card by fraudulent means)
- AR Stat. Ann. Sect. 41-2308 (1977)
- GA Code Ann. Sect. 26-1705 to Sect. 26-1705.10
- HI Rev. Stat. Sect. 851-10
- IL Ann. Stat. Ch. 121 1/2, Sect. 60 Ch. 121 1/2, Sect. 601 et seq. (Supp. 1978)
- IN Code Ann. Sect. 35-43-51 to 35-43-55 (1979)
- IA Code Ann. Sect. 715.1 to 715.6 (West Supp. 1978)
- KS Crim. Code & Code of Crim. Proc. Sect. 16.841-16.844 (1974)
- KY Rev. Stat. Sect. 434.550-434.730 (Supp. 1978)
- LA Rev. Stat. Ann. Sect. 14.67 (1974)
- ME Rev. Stat. Tit. 17-A Sect. 905 (Supp. 1978)
- MD Crim. Law. Code Ann. Sect. 145 (Supp. 1978)
- MN Stat. Ann. Sect. 609.52 (West Supp. 1979)
- MT Rev. Code Ann. Sect. 94-6-307 (Supp. 1974)
- NV Rev. Stat. Sect. 205.610-205.810 (1977)
- NM Stat. Ann. Sect. 30.16.24-30.16-38 (1978)

- NC Gen. Stat. Sect. 14-113.8-.17 (Supp. 1977)
- OH Rev. Code Ann. Sect. 2913.21 (Supp. 1978)
- SC Code Sect. 16-13-270 and 280 (1976)
- RI Gen. Laws Sect. 11-49-12 to 13 (Supp. 1978)
- SD Compiled Laws Ann. Sect. 22-30 A-8.1 (Supp. 1977)
- UT Code Ann. Sect. 76-6-506.3 (1978)
- WI Stat. Ann. Sect. 943.41 (West Supp. 1979)
- WA Rev. Code Ann. Sect. 9A.56 (1977).

Whether these may be used to prosecute will depend on the pattern of facts and the statutory language. For example, in some jurisdictions, uttering a fictitious account number is enough to trigger the law. See, for example, Del. Code Ann. Title 11, Sect. 904 (1975) ("credit card" includes writings, numbers, or other evidences of undertaking to pay for property). In other jurisdictions, the actor must actually "utter a fictitious card"; thus, an account number system where no credit cards are actually issued probably would not trigger the statute. See, for example, Va. Code Ann. Sect. 18.1-125.2(2) (Supp. 1974) ("credit card" means instrument or device).

3. Theft by Deceit

In a Missouri case, *State* vs. *Hamma* [569 S.W.2d 289 (Mo. Ct. App. 1978)], decided before the passage of the Financial Institutions Regulatory and Interest Rate Control Act (FIRA), the defendant was accused of stealing by deceit. On appeal he contended that the information did not state conduct constituting the crime charged. The defendant was accused of intentionally stealing $800 by deceit by obtaining someone else's automatic teller bank card and secret identification number and taking money out of the machine at $50 each withdrawal. The defendant contended that he made no representation, let alone a fraudulent representation, and argued that the offense required a verbal misrepresentation to the party defrauded. The court rejected that argument, stating that a misrepresentation could consist of any act, word, symbol, or token calculated and intended to deceive. The court held that the deceit may be made either expressly or by implication. Moreover, the court held that the fraudulent manipulation of an automatic teller is analogous to the use of stolen credit cards, and it cited an earlier D.C. case, *Hymes* vs. *U.S.* [260 A.2d 679 (D.C. App. 1970)] as precedent.

In a Virginia case, *Lund* vs. *Commonwealth* [217 Va. 688, 232 S.E.2d 745 (1977)], the defendant was charged with theft of keys, computer cards, and computer printouts from a university and using, without authority, computer operation time and services with intent to defraud. The defendant was a graduate student in statistics and a Ph.D. candidate whose dissertation required the use of the computer. He used over $26,000 worth of computer time. The defendant contended that the conviction of grand larceny was faulty because there was no evidence that the articles stolen (e.g., keys, cards, and printouts) were worth over $100 and that computer time and services were not subjects of larceny. The court agreed, holding that the phrase "goods and chattels" could not be interpreted to include computer time and services in view of the rule that criminal statutes must be strictly construed. Moreover, the court held that the unauthorized use of the computer was not the subject of larceny because nowhere in the criminal code section was the word "use" used. The court cited a 1927 case that held that the use of the machinery in spinning facilities did not constitute larceny.

Finally, the Commonwealth contended that although the printouts had no market value, they should be valued by the cost of labor and materials to produce them. The court rejected that argument and also stated that if there was no market value, the only value that could be used was actual value and in this case the only actual value was to the defendant. The court compared *Hancock* vs. *State* [402 S.W.2d 906 (Tex. Crim. App. 1966)] (theft of a computer tape containing a valuable program), where the criminal statute was sufficient upon which to base a conviction and the program stolen had a monetary value.

4. Forgery

To obtain access to another's computer system, the actor will need to discover and use the owner's confidential entry code to the system and account number. The use of this false entry code for the purpose of defrauding or injuring any party may be forgery. Although jurisdictions that have retained the common law requirements of a signature and document would not be applicable, a number of jurisdictions have expanded the common law scope of the crime so that any making, altering, executing, completing, or authenticating of any seal, signature, writing, or symbol of right, privilege, or identification that may defraud or injure another is forgery.

The California Penal Code [Sect. 470 (West 1970)] provides, interalia, that anyone who "...counterfeits or forges the seal or handwriting of another..." is guilty of forgery. The central question is whether the entry code is either a seal or a signature. The entry code is analogous to the signature on a check (itself a form of computerized draft that uses optical character readers) or the authenticating seal of a notary or official. Moreover, in *People* vs. *Burkett* [271 Cal. App. 2d 130, 74 Cal. Rptr. 692 (1969)], the court held that "seal or handwriting" was a "catchall," broad enough to include a photocopy of a reproduction of a seal and a facsimile signature. The defendant had used photocopies of dollar bills in dollar bill changers [271 Cal. App. 2d at 134, 74 Cal. Rptr. at 694].

The New York forgery statute [N.Y. Penal Law Sect.

170.00 et seq. (McKinney 1967)] is a statutory, not common law, offense and covers any false making of private writings that might operate to the prejudice of another.

Delaware, Texas, and Pennsylvania have similar forgery statutes, apparently patterned after the Model Penal Code. Each includes, as protected writings, any symbols of "value, right, privilege, or identification." [Pa. Stat. Ann. Title 18, Sect. 4101(b) (1973); Del. Code Ann. Title 11, Sect. 863 (1975); Tex. Stat. Ann., Penal Code Sect. 32.21 (a)(2)(c) (1974).] The offense is a felony in Texas and Delaware and a misdemeanor of the first degree in Pennsylvania.

Thus, at least in some jurisdictions, the use of a false entry code, a symbol of right, privilege, and identification that prints out on any machine and is used to defraud or injure is forgery. As noted in conjunction with credit card abuse, the prosecutor will need to prove a fraud or injury, actual or intended, to trigger the statute. Even though it seems logical that any pecuniary loss should be sufficient, the prosecutor may want to charge at least one of the various theft charges applicable in that proof of value then would not be at issue.

5. Obliteration or Bugging of Programs

Obliteration or bugging of programs is a form of computer abuse that can be broadly characterized as criminal or malicious mischief. Whereas most jurisdictions have criminal mischief statutes of one type or another that proscribe physical damage to another's personal property, some also have "interference with use" statutes that make it a crime to tamper or interfere with another's property so that the person suffers loss.

a. Physical Damage

As long as prosecutors successfully characterize the damage, they should have no difficulty when the outward appearance of the disk or tape is unchanged. The problem of successful characterization in California should be minimized by *People* vs. *Dolbeer* [214 Cal. App. 2d 619, 29 Cal. Rptr. 573 (1963)]. California's malicious mischief statute, Cal. Penal Code Sect. 394 (West 1970), provides that any malicious injury or destruction of personal property of another is a misdemeanor.

Five other jurisdictions—Massachusetts [Mass. Gen. Laws Ch. 266, Sect. 127 (1968)]; Delaware [Del. Code Ann. Title 11, Sect. 811(a)(1)(1975)]; the District of Columbia [D.C. Code Sect. 22-403 (1967)]; Florida [Fla. Stat. Ann. Sect. 806.13 (Supp. 1976)]; and Virginia [Va. Code Ann. Sect. 18.1-172 (Supp. 1974)]—have malicious or criminal mischief statutes virtually identical to that of California. Penalties generally vary according to the amount of damage (except in Virginia), and large amounts of damage may give rise to felony charges in Delaware and Florida and felony-level punishment in Massachusetts and the District of Columbia.

Unlike the jurisdictions discussed above (which deal with tangible or personal property), New York's criminal mischief statutes use the general word "property" [N.Y. Penal Law Sect. 145.00 et seq. (McKinney 1967)]. But New York [N.Y. Penal Law Sect. 155.00(1)] defines property subject to theft as "money, personal property, or . . . thing in action, evidence of debt or contract, or any article, substance or thing of value." Property for purposes of the criminal mischief and tampering statutes means tangible property. [See R. Denzer and P. McQuillan, Practice Commentary Sect. 145.00, N.Y. Penal Law (McKinney 1967) citing *Polychrome Crop.* vs. *Lithotech Corp.* 4 App. Div. 968, 168 N.Y.S. 2d 346 (1957) (predecessor to current criminal mischief statute not intended to apply to violations of incorporeal rights).] Thus, although the statute differs slightly from the California statute, the characterization problem is the same.

The New Jersey malicious mischief statutes [N.J. Stat. Ann. Sect. 2A; 122-1 and 17036 (1969)] use differing descriptions of the thing protected; whereas the former refers to personal property, the latter refers to property.

In *State* vs. *Shultz* [41 N.J.L.J. 176, 177 (1918)], a lower court emphasized that "in order that the offense of malicious mischief may be perpetrated, it is necessary that there be injury to property; but . . . it is not necessary that the property be entirely destroyed." The operation of the New Jersey malicious mischief statute is unique among all the jurisdictions surveyed. When any malicious mischief occurs, the prosecutor charges a misdemeanor [N.J. Stat. Ann. Sect. 2A; 122-1 (1969)]. But if the prosecutor fails to prove that the value of the property damaged was more than $200, the defendant cannot be convicted of a misdemeanor, but can only be adjudged a disorderly person, punishable by up to 6 months in jail and/or a fine up to $500 [*State* vs. *Tonnisen*, 92 N.J. Super. 452, 224 A.2d 21 (1966)].

Pennsylvania's criminal mischief statute is generally inapplicable because Pa. Stat. Ann. Title 18 Sect. 3304(a) (1) and (2) are limited to destruction by dangerous means or so as to cause danger to person or property. However, Subsection (a)(3) appears to incorporate theft by false pretenses and extortion into criminal mischief, perhaps as a smaller included offense of theft. As such, it would be applicable where any loss was caused and the actor used deception to accomplish the mischief. Criminal mischief may be a summary offense, misdemeanor, or felony depending on the amount of loss [Pa. Stat. Ann. Title 18, Sect. 3304(6)].

Two Texas statutes may be relevant in the case of damage to programs. The Texas criminal mischief statute [Tex. Stat. Ann., Penal Code Sect. 28.03 (1947), Subsection

(a)(1)] provides that damage or destruction of tangible property of another is an offense. That is not unusual. However, Texas law also proscribes any alteration or destruction of a writing with intent to defraud. While the law resembles the forgery statute in its scope, it extends to any alteration irrespective of what the writing purports to be. [See Tex. Stat. Ann., Penal Code Sect. 32.47 (1974).] Thus, so long as the damage is to printed programs, this provision would be applicable.

The Illinois criminal mischief statute [I11. Ann. Stat. Ch. 38, 21-1 (Smith-Hurd 1970)] specifically proscribes damage to articles representing trade secrets. The statute provides that knowing damage to property of another is an offense. Property is defined as "anything of value," including articles representing secret scientific information, and this definition applies to all offenses against property. The offense is punishable by up to 5 years in prison and a fine up to $500 if the value of the program damaged exceeds $150.

b. Interference with Use

Aside from the Pennsylvania statute, which might be used in a tampering situation but does not specifically refer to interference with use as a crime, Pa. Stat. Ann. Title 18, Sect. 3304(a)(3) (1973), statutes in four other jurisdictions make criminal tampering a punishable offense.

Under the general rubric of criminal trespass, the California Penal Code, Sect. 602(j), provides that entry of lands with intent to interfere with any lawful business is a misdemeanor. New York has abroad array of antitampering statutes. N.Y. Penal Law Sect. 145.20 (criminal tampering in the first degree, a Class D felony) would be applicable to any tampering with a publicly owned computer operation. That statute contains a broad provision, Sect. 145.15(1) (criminal tampering in the second degree, a Class B misdemeanor) that applies to any tampering with any property that causes substantial inconvenience. It is also a Class B misdemeanor to create a risk of substantial damage to property whether or not such damage occurs. Substantial damage is defined as damage in excess of $250.

Texas has an analogue to the New York antitampering statute, Tex. Stat. Ann., Penal Code 6 28.03(a)(2) (1974). A violation is a Class C misdemeanor if the tampering caused substantial inconvenience of no ascertainable monetary amount, and a misdemeanor or felony if the amount of loss is calculable. The Virginia statute [Va. Code Ann. Sect. 18.1-183 (Supp. 1974)] is similar to the California criminal trespass statute discussed above but, unlike the California law, specifically extends its scope to any interference "with the rights of the owner, user, or the occupant thereof..." As in California, the offense is a misdemeanor.

6. Misappropriation of Programs

Computer abuse in this category of misappropriation of programs may take several forms: (a) unauthorized or fraudulent access to programs by an unprivileged user of a facility or by a privileged user of the facility who has no authorized access to the programs; (b) unauthorized or fraudulent disclosure of proprietary programs by an employee, former employee, or contract program developer. The leading reported case of this category is *Hancock* vs. *State*, 1 CLSR 562, 402 S.W.2d 906 (Tex. Crim. App. 1966). In *Hancock*, the defendant-employee offered a listing of 59 programs for sale to a person he thought was an agent of one of his employer's clients.

The scope of state criminal laws protecting programs is often determined by whether the programs are included with property otherwise subject to protection. An initial question is whether unpatented and uncopyrighted programs may be protected by criminal trade secret laws. In states that have no trade secret laws, or where dual charges of larceny and theft of trade secrets may be maintained [see, for example, *Ward* vs. *Superior Court*, 3 CLSR 206 (Memorandum opinion 51629, 1972)], the prosecutor must determine whether programs are property subject to larceny. In states that have no criminal trade secret laws, the prosecutor must often look to general "offenses against property" statutes to punish the type of computer abuses noted above. Such general statutes are almost the exclusive remedy in all states for obliteration or bugging.

Computer programs, a form of intangible intellectual property, should be protected by state criminal laws. For excellent discussions of the inadequacy of civil remedies, see Comment, Industrial Espionage: Piracy of Secret Scientific and Technical Information, 14 U.C.L.A. L. Rev. 911, 927 (1967), and Comment, Protection of Trade Secrets in Florida, 24 U. Fla. L. Rev. 721 (1972). First, without protection, a program developer has little incentive for creating and investing. Second, it is only just that laborers enjoy the fruit of their labors. Third, the criminal law must prevent misappropriation, misuse, and distortion of proprietary programs. See Galbi, Copyright and Unfair Competition, 3 CLS Sect. 4-3, Art. 1, and Bender, Trade Secret Protection of Software, 38 Geo. Wash. L. Rev. 51629(1972).

With the exception of trade secrets laws, almost all state offenses against property statutes antedate the advent of computers. Definitions and case interpretations may make prosecution for abuse of an intangible difficult. For instance, abuse of programs by copying or unauthorized communication may be seen as a mere disclosure of an idea. Malicious mischief may be deemed only a rearrangement of magnetic discontinuities with no requisite

damage or destruction to the tangible property carrying the programs.

Whether a particular abuse may be successfully prosecuted under larceny or malicious mischief statutes may turn on the skill of the prosecuting attorney in framing the charge where a person has misappropriated programs contained on a magnetic tape or on a printout. *Hancock*, 1 CLSR 562, 402 S.W.2d 906 (Tex. Crim. App. 1966), shows that so long as the value of the intangible intellectual property is added to the value of the tape or paper (a reasonable addition in that it is doubtful that the tape or paper would have been stolen but for the program value) an indictment or information charging grand larceny should be upheld against a motion to dismiss. A closer question might concern the actor who was ignorant of the program's existence but set out to steal bulk paper or computer tapes per se. The general rule appears to be that the prosecution is not required to prove knowledge of value by the thief [see, for example, *People* vs. *Earle*, 222 Cal. App. 2d 476, 35 Cal. Rptr. 265 (1963)], and that the market value is fair market value to disinterested buyers and sellers. See also *People* vs. *Dolbeer*, 214 Cal. App. 2d 619, 623, 29 Cal. Rptr. 573, 575 (1963) (the value of telephone company customer lists is determined by "effort...efficiency...and... secrecy...," not the paper alone).

Where an actor obliterates or bugs programs by altering the magnetic tape or printout, the prosecutor must urge that the "property" that was "injured" under the common form of malicious mischief statutes was the tangible tape or paper. What gives the paper or tape value is the program [see *Hancock* vs. *Decker*, 1 CLSR 858, 379 F.2d 552 (5th Cir. 1967)]; when one obliterates the program he obviously injures the tape by rendering it unfit for its purpose. Just as in larceny prosecutions, the prosecutor must be careful to characterize the conduct so as to bring it within the statutory proscription, for example, (1) the thing injured was a tanglible tape, and (2) the injury was the obliteration of the program. This method of characterization was suggested by John Kaplan, former prosecuting attorney, currently Professor of Law, Stanford School of Law.

Only in two instances will the abuse of programs probably be unprotected under common larceny statutes. First, where the actor copies a program on his own paper or tape and asports the copies but leaves the originals, he has not committed common law larceny as interpreted in most jurisdictions. But see *Ward* vs. *Superior Court*, 3 CLSR 206 (Memorandum opinion 51629, 1972, sustaining a grand theft charge under a similar fact pattern). The result in *Ward* is logical, since one who asports a copy of a program steals both value and control of the property. But the fact that so many states have found a need specifically to proscribe copying a trade secret, Cal. Penal Code Sect. 499c(b)(3)-(4) (West 1970), demonstrates how resistant most courts have been to accepting value or control theories as equivalent to the more traditional "permanent deprivation" theory of larcenous intent.

Second, when a person takes knowledge or electronic signals, he has probably not committed larceny within common law statutes. In *Ward* vs. *Superior Court* [Ward 1973], Judge Sparrow stated that electronic impulses "...are not tangible and hence do not constitute an 'article' capable of being stolen within California's trade secrets law" [3 CLSR 205, 208 (Memorandum opinion 51629, 1972)]. This opinion may well represent the popular perception of electronic impulses as outside the scope of property protected by statute. As to theft of knowledge, theses that ideas may not be stolen seems to preclude prosecution of those who develop a program and use the knowledge gained thereby for a competitor or for themselves. But see Tex. Stat. Ann., Penal Code Sect. 31.05(b)(3) (1974) (any communication or transmission of a trade secret without consent is a felony of the third degree).

When actors misappropriate computer programs stored in a computer, they may run afoul of several other types of laws. First, the state may denominate misappropriation of trade secrets as a separate and distinct offense. Second, notwithstanding trade secrets laws, the actors may be guilty of larceny; as a corollary, the recipients of the program, other than the actors, would be receiving stolen goods. Third, the offender may have committed one or more of the crimes set forth above.

7. Trade Secrets

The Restatement test of a trade secret is that the process, item, etc., be used in the trade or business, be kept secret, and give the owner a competitive advantage over those who do not know it. Trade secret misappropriation statutes are enormously useful in cases of program theft but should be analyzed carefully to make sure the technical requisites have been met. [For example, in *Ward* (1972), the judge held that the transference of electronic impulses did not constitute a taking.]

Larceny statutes are relevant in three different contexts related to trade secrets. First, in states that have misappropriation of trade secrets as a separate and distinct offense, a dual charge of larceny and theft (or abuse) of trade secrets may arise from the same act [cf. *Ward* vs. *Superior Court*, 3 CLSR 206 (Memorandum opinion 51629, 1972)]. This does not mean, however, that double punishment may be meted out when an actor engages in a single, indivisible transaction that may encompass several crimes. Only the single, heaviest punishment of all the crimes may be imposed. The critical question is what constitutes a single indivisible transaction. Second, where theft of trade secrets is subsumed into the general larceny statute, the burden of

the prosecutor to prove trade secrets as property subject to larceny is eliminated. Third, even where trade secrets have not been statutorily included as property subject to larceny, the prosecutor may be able to prove that the secret is a "thing of value."

The New York larceny statute, N.Y. Penal Law Sect. 155.30 (McKinney Supp. 1974), is an excellent example of how a jurisdiction may include trade secrets, "secret scientific material," in its larceny statute. Both stealing and copying are separate offenses, each a Class E felony. If the trade secret has a readily ascertainable value (market or replacement value, see Sect. 155-20) in excess of $1,500, the prosecutor may desire to waive prosecution under Sect. 155.30 and instead charge second degree grand larceny, Sect. 155.35, a Class D felony punishable by 1 to 7 years in prison and a discretionary fine similar to that for Class E felonies.

Unlike New York law, the California theft statute, Cal. Penal Code Sect. 48a (West 1970), nowhere specifically includes trade secrets as property subject to theft. Whereas the trade secret provision, Cal. Penal Code Sect. 499c (West 1970), is probably the exclusive sanction for copying a trade secret without asportation, [cf. *Bender*, Trade Secret Protection of Software], the *Ward* [1972] case indicates that a dual charge of theft and theft of trade secrets is maintainable where an article representing a trade secret, or a copy thereof, is asported.

Although New York is the only state that has incorporated trade secrets into both its own and a general larceny statute, at least three states (Pennsylvania, Massachusetts, and Illinois) have incorporated trade secret protection into theft or larceny statutes without denominating abuse of trade secrets as a separate offense from theft or larceny generally. Ordinarily, trade secret protection can be incorporated into theft or larceny statutes in three ways: (1)c onsolidation of theft of trade secrets into a theft or larceny statute, as in Pennsylvania; (2) definition of trade secret theft as larceny, as in Massachusetts; or (3) including of trade secrets in lists or property protected by larceny statutes, as in Illinois.

8. Privacy Invasions

Almost every state has one or more statutes proscribing invasions of privacy by persons in the public sector. Bills, pending in some states, may affect the private sector as well. Some of these statutes carry criminal penalties that may be invoked when an unauthorized and willful disclosure of personal information is made from a computer database.

C. Federal Penal Laws

The most important federal laws for prosecuting computer crime and computer-related crime are the Communications Fraud and Abuse Act of 1986, the Electronic Communications Privacy Act of 1986, the Credit Card Fraud Act of 1984, the Federal Copyright Act of 1976, and the Wire Fraud Act. These laws are briefly analyzed below.

1. Computer Fraud and Abuse Act of 1986

The Computer Fraud and Abuse Act of 1986 [18 U.S.C., Ch. 47, Sect. 2101-2103, Sect. 1030 Fraud and Related Activity in Connection with Computers] is the result of many tortuous years of producing draft bills in both houses of Congress. The final adopted version, the result of a compromise between the U.S. Department of Justice and two House of Representatives committees, covers only limited-forms of computer abuse. The U.S. Secret Service, in addition to the FBI, has been given explicit jurisdiction to investigate the six offenses specified in the statute, which involve "knowingly and intentionally access[ing] a computer without or exceeding authorizationand thereby"

(1) Obtaining restricted military foreign relations or atomic energy information to be used to injure the United States.

Penalty: Fine and/or 10 years in prison (20 years if repeated offense).

(2) Obtaining information in financial or consumer credit records from financial or credit-reporting institutions.

Penalty: Fine and/or 1 year in prison (10 years if repeated offense).

(3) Affecting the use of a U.S. government or contractor computer.

Penalty: Fine and/or 1 year in prison (10 years if a repeated offense).

(4) Furthering a fraud or obtaining anything of value excluding usage in a financial institution or U.S. government computer.

Penalty: Fine and/or 5 years in prison (10 years if repeated offense).

(5) Altering, damaging, using, or destroying information in or prevents authorized use of a financial institution or U.S. government computer causing more than $1,000 loss or loss in personal medical care.

Penalty: Fine and/or 5 years in prison (10 years if repeated offense).

(6) Trafficking in any password or similar information for unauthorized computer access if it affects interstate or foreign commerce or the U.S. government.

Penalty: Fine and/or 1 year in prison (10 years if a repeated offense).

By a memorandum of understanding, the FBI currently has jurisdiction over cases involving national security, terrorism, banking, and organized crime. The Secret Service has jurisdiction over all other cases.

Accessing a computer is defined only in terms of exceeding authorized access; otherwise, accessing is not defined and could mean merely dialing a telephone number assigned to the input port of a dataswitch or computer. The definition might also require a computer acknowledgment that facilitates the use of the computer by the person authorized to use it.

"Without or exceeding authorization" puts the onus of defining an offense on the owner or management of a computer. Therefore, an investigator or prosecutor must obtain information on exactly what is authorized and not authorized in a particular computer environment. For example, policy concerning personal use of an employer's computers determines whether using the computer for other than employer-specified purposes is an offense.

The definitions of the six offenses have raised several questions. Offense #3 involving use of a computer is so wide-ranging that materiality may be questioned. Offense #5 poses the problem of identifying the monetary loss; that could involve determining the computer usage rates, as well as the consequential losses associated with the act (e.g., lost staff time, replacement cost of destroyed or damaged information). Offense #6 is aimed in part at electronic bulletin board system operators and users; questions may arise about user IDs that may be public in one system but confidential in another.

The statute contains only one technical definition. A computer is defined as "an electronic, magnetic, optical, electro chemical, or other high-speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator or similar device." The use of the terms "computer program, "software," "computer system," and "computer network" often found defined in state laws are absent from the federal statute.

This definition of computer may cause considerable difficulties for prosecutors, especially as the technology advances and changes. Data storage and communications facilities probably mean connected equipment rather than physical facilities such as a computer media vault. The exclusion of automated typewriters or typesetters is particularly vexing; presumably, these exclusions were meant to restrict application of the statute to the publishing industry. Excluding a portable hand-held calculator may be appropriate today, but in the near future portable hand-held calculators will probably be more powerful than today's microcomputers. Technical definitions generally tend to make criminal statutes obsolete. The complete text of the federal statute is included in Appendix A.

2. Electronic Communications Privacy Act of 1986 (18 U.S.C.; Ch. 65 Sect. 1367; Ch. 119, Sect. 2510-2521; Ch. 121, Sect. 2701-2710; Ch. 206, Sect. 3121-3126)

The 1986 Electronic Privacy Act extends the current privacy guarantees for traditional telephones to communications involving cellular phones that operate by high-frequency radio waves, transmissions by private satellite, paging devices, and messages transmitted and stored in computers, known as "electronic mail." The law expands and updates 1968 legislation (PL 90-351) that specifies when and how the government can wiretap conventional telephones, but says nothing about new forms of communication that use more modern forms of technology to transmit messages.

While Justice Department officials realized there were gaps in the law, they were initially reluctant to tamper with the statute for fear of weakening the department's ability to use wiretaps as a law enforcement tool. But the electronics industry helped convince Justice that the law had to be amended to deal with technological change and to make their products more marketable.

The basic premise behind the legislation is to protect the content of private communications, regardless of the means of transmission. The law includes the following major provisions:

a. Definitions and Exemptions

- Rewrote the 1968 wiretap law to protect "electronic communications" and "electronic communications system."
- Defined electronic communications to include "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature that is transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce."

- Defined electronic communications system to mean any wire,radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.
- Exempted from coverage—and thus left unprotected from intrusion—any radio communication that is "readily accessible to the general public."

  Also exempted were the radio portion of a cordless telephone communication, which is transmitted between the cordless telephone handset and the base unit, any communication made through a tone-only paging device, communications between amateur radio operators, general mobile radio services, marine and aeronautical communications systems, police, fire, civil defense and other public safety radio communications systems, and specified satellite transmissions.
- Protected radio signals in several instances: if the signal were scrambled or put into code, that is "encrypted"; if the signal's frequency were changed to one withheld from general use by the Federal Communications Commission (FCC); if the signal were transmitted through a common carrier, like a cellular telephone company that serves the public; or if the signal were transmitted via specific radio frequencies set out in the bill.

b. Private Interception

- Made it illegal for individuals to intercept electronic communications as defined in the bill.
- Made the offense a felony with a penalty of a fine, a prison term of up to 5 years or both when the interception is for any illegal purpose, such as gathering stock information for insider trading, is for direct or indirect commercial gain, or is an interception of a scrambled or encrypted signal.

  Generally, when the interception is of a radio communication, the penalty would be a maximum prison term of 1 year and/or a fine. There are three exceptions: when the interception involves the radio portion of a cellular phone call, specified mobile radio services, or a paging service. In these instances,the violation would bring only a $500 criminal fine.
- Required the government to prove that a defendant intentionally sought to intercept protected communications.
- Established a reduced penalty structure for individuals who intercept satellite transmissions for private use. A first offender would be fined $500 and the government could sue to halt the interception. If an injunction were granted, the judge could then use several means to enforce the order, including citing the defendant for civil or criminal contempt for failure to obey the order.
- Provided a $500 fine for the second and any subsequent offense.
- Authorized the person whose communication was intercepted to sue the alleged perpetrator in federal court.
- Authorized a damage award of the greater of actual damages or statutory damages from $50 to $500 on the first offense, and of actual damages or statutory damages between $100 and $1,000 on the second offense.
- Provided for stiffer penalties when the interception was for commercial advantage or illegal purpose, such as to intercept stock information for insider trading. The violator could be ordered to pay the greatest of $10,000, $100 for each day of the violation or the sum of actual damages suffered by the plaintiff and any profits made as a result of the violation.
- Made it illegal for a person or entity providing wire or electronic communications service to the public to divulge knowingly the contents of any communication except to the person sending the information or to the intended recipient.
- Allowed disclosure of a communication with the consent of the originator or recipient to a law enforcement agency when it appears a crime has been committed.

c. Government Interception

- Allowed the government to intercept electronic communications after obtaining a court order. Judges could grant the order after they had determined that the interception "may provide or has provided" evidence of any federal felony.
- Allowed law enforcement officials to get court approval for a"mobile tracking device" that goes beyond the geographic jurisdiction of the court. The only proviso is that the device, which is used to track a moving suspect, be installed in the jurisdiction of the judge who approved the order. (Federal courts are divided by geographic region within the 50 states and selected federal territories.)
- Expanded from the 1968 law the list of officials who can seek a court order and expanded the number of crimes for which an interception is authorized.

- Gave the government the right, in limited circumstances, to obtain a roving telephone tap that would enable tapping several phones. Under current law, the government is required to specify which phone officials are going to tap. The government would have to explain why specifying a particular phone "is not practical."
- Made it a felony for any person to divulge information about a possible communication interception by the government in order to obstruct, impede, or prevent such interception.

d. Stored Communications

- Protected the privacy of stored communications, either before or after delivery if a copy is kept.
- Made it a misdemeanor to break into any electronic system holding copies of messages either before or after delivery or to exceed authorized access in the system to alter or obtain the stored messages.
- Provided a fine for a first offense of up to $250,000, a maximum 1-year prison term or both, if the offense were committed for commercial advantage of "malicious destruction or damage." There would be a 2-year prison term for a second offense.
- Provided a maximum fine of $5,000 or imprisonment of up to 6 months for an offense that was not for commercial gain or for malicious destruction or damage.
- Allowed the government to require disclosure of copies of electronic mail, no matter how long it has been stored, if the government obtained a warrant.
- Gave the government the additional option of using a subpoena to get information when the information has been stored more than 6 months. To do that, it must give prior notice to the electronic-mail customer involved. In addition, the subpoena must be issued by a government agency authorized by statute to do so or by an agency acting at the request of a grand jury.
- Required that the court order shall be issued only if the governmental entity shows that there is reason to believe the contents of the electronic communication or the records are "relevant to legitimate law enforcement inquiry."
- Gave the electronic-mail customer the right to file a motion to quash any subpoena or vacate any court order. The person seeking to block the subpoena or court order would have to show that the records sought "are not relevant to a legitimate law enforcement inquiry" or that the government had not complied with the procedures established for obtaining information.

e. Pen Registers; Trap and Trace

- Established standards for government use of "pen registers" and "trap and trace devices."
- Defined a pen register as a device that records or decodes numbers dialed or otherwise transmitted by telephone. However, devices used to monitor calls for billing or recording incident to billing are not covered.
- Defined a trap and trace device as one that captures an incoming electronic or other impulse and can identify the number from which a call was made.
- Barred generally the use of pen registers and trap and trace devices except pursuant to a court order.
- Provided a penalty for knowingly violating this section of a fine and imprisonment of up to one year or both.
- Required a government agency seeking a court order to use a penregister or trap and trace device to certify that the information "likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applying government agency."
- Specified the elements a court-order granting approval for a penregister or trap and trace device must contain. The order must include the identity of the person whose phone will have the penregister or trap and trace device attached to it, the identity of the person who is the subject of the investigation, the number and physical locations of the telephone lines to be monitored and a statement of the offense to which the information obtained is expected to release.
- Limited the use of the device to 60 days, although 60-day extensions could be granted upon application.
- Specified that the order approving installation of a penregister or a trap and trace device shall be sealed until otherwise ordered by the court.
- Required that the provider of the wire or electronic communications service to be monitored cooperate with law enforcement agencies in installing the pen register or trap and trace device.
- Required that the provider of such service be "reasonably compensated for reasonable expenses" for his cooperation and facilities.

3. The Credit Card Fraud Act of 1984 (18 U.S.C. Ch. 47, Sec. 1029)

This law was enacted primarily in the interest of controlling credit card fraud and card counterfeiting. Because the definition of credit card is broad, the law covers many

computer-related offenses. The objects of the offenses are "access devices," which are defined as "any card, plate, code, account number, or other means of account access that can be used alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value or that can be used solely to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." Therefore, the following access devices could be included as the object or tool of an offense:

- Magnetic stripe credit card
- Smart card
- Credit plate (containing an address)
- Dynamic password card
- Key
- Any shaped device for machine insertion
- Account balance or state of account
- Computer access protocol data
- Unlisted telephone number
- Computer user ID
- Computer password phrase
- Computer password
- Cryptographic key
- Computer account number
- Answers to a question or series of questions
- Banking account number
- PIN (personal identification number)
- PAN (personal account number)

The exclusion of devices associated with paper instruments in funds transfer would presumably exclude document seals, wax seals, and stamps. Any knowable, but private information used for access to computers seems to be included.

In a computer crime context, the offenses include the following:

(1) Fraudulently producing, using, or trafficking in one or more counterfeit devices.

(2) Fraudulently trafficking in or using one or more unauthorized devices and obtaining anything of value aggregating $1,000 or more during a one-year period.

(3) Fraudulently possessing 15 or more counterfeit or unauthorized devices.

(4) Fraudulently producing, trafficking in, having control or custody of, or possessing device-making equipment.

Punishment ranges from $10,000 to $100,000 or 10-20 years in prison. Multiple convictions increase penalties.

This law may be used against deceitful hackers and pirate bulletin board system operators who search for, test, and exchange computer access telephone numbers, user IDs, passwords, and access protocols for computer intrusion. The law is also applicable to a wide range of computer intrusion activities in the federal jurisdiction.

4. Federal Copyright Act of 1976

Theft of computer programs can be prosecuted under federal copyright laws. The copyright office has accepted registration of computer programs as "books" since 1964. The House Committee Report on the Copyright Act of 1976, p. 54, states that the term "literary works . . . includes computer data bases, and computer programs to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves." Thus authors of computer programs can protect documentation and lines of computer code from copying, but copyright protection does not extend to programmers' algorithms.

In addition to providing for civil actions and damages for copyright infringement, the Copyright Act of 1976 also provides for criminal penalties for infringement and for fraudulent removal of copyright notice. Criminal liability for infringement is proven by showing the elements of civil infringement, ownership in another party and copying, and, in addition, by demonstrating willfulness and financial gain [17USC Sect. 506(2)]. Section 506(a) provides for a maximum penalty of 1-year imprisonment and a $10,000 fine. Section 506(b) also provides for a mandatory forfeiture and destruction of all infringing copies.

Section 506(d) makes it a criminal act to remove or alter any notice of copyright with a fraudulent intent. This conduct is criminal even though it creates no civil liability. Anyone convicted of such an act is subject to a $2,500 fine.

State laws purporting to describe criminal or lawful conduct involving copyright infringement under federal laws are invalid under the doctrine of federal preemption.

5. Wire Fraud Act (18 U.S.C. Sect. 1343)

The elements of Sect. 1343 are identical to Sect. 1341, with the exception of the federal medium abused. When one uses a remote terminal to perpetuate a computer fraud, or when one telephones an accomplice, so long as the "message" crosses state lines, the statute is applicable. All reported cases involving Sect. 1343 have dealt with conversations that crossed state lines, leading one to believe that the message must, in fact, cross state lines. Since Sect. 1343 does not use the word "facility," jurisdiction hinges on use of an interstate wire, notwithstanding the fact that "[i]t cannot be questioned that the nation's vast network of telephone lines constitute interstate commerce" [*United States* vs. *Holder*, 302 F. Supp. 296, 298 (D. Mont. 1969)]. It is not clear that the use of the word "facility" in any new legislation would embrace interstate calls either; see *United States* vs. *DeSapio*, 299 F.Supp. 436, 448 (S.D.N.Y. 1969) (construing phrase "facility in . . . interstate commerce" as requiring interstate calls for 18

U.S.C. Sect. 1952), because there may be a distinct difference between facilities "in" interstate commerce and facilities "of" interstate commerce. Both mail fraud and wire fraud are very useful aids to the prosecution of computer crime.

6. Other Federal Authority Bearing on Computer Crime

a. Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA)

Title XX of FIRA, the Electronic Fund Transfer Act, is designed to define and provide for individual consumer rights as they are affected by electronic funds transfer (EFT). In so doing, the act provides federal regulation of EFT by establishing the rights, liabilities, and responsibilities of participants, including financial institutions, consumers, and other users of EFT.

Section 916 of the act is the criminal liability section, which most directly concerns or at least may have a bearing on computer crime in the federal arena. It provides for a fine of not more than $5,000, imprisonment for not more than 1 year, or both for anyone who knowingly and willfully gives false information or fails to provide information required by the act or regulations promulgated thereunder, or otherwise fails to comply with the act or its regulations.

The second section of the criminal liability provision imposes a fine of not more than $10,000, imprisonment for not more than 10 years, or both for the following six acts when interstate or foreign commerce is involved, when the money, goods, services, or things of value involved have a value of $1,000 or more when aggregated over a 1-year period and when a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument is involved. The term "debit instrument" means a card, code, or other device by which a person may initiate an EFT. The six acts include:

- Knowingly using or attempting or conspiring to use a debit instrument, as described above, to obtain anything of value, as described above.
- With unlawful or fraudulent intent, transporting or attempting or conspiring to transport a debit instrument knowing that it is counterfeit, stolen, etc.
- With unlawful or fraudulent intent, using an instrumentality of interstate or foreign commerce to sell or transport a debit instrument knowing it is counterfeit, stolen, etc.
- Knowingly receiving, concealing, using, or transporting anything of value (except tickets for interstate or foreign transportation) which has moved in interstate or foreign commerce and has been obtained with a counterfeit, stolen, etc., debit instrument.
- Knowingly receiving, concealing, using, selling, or transporting one or more tickets for interstate or foreign transportation whose value aggregated within a 1-year period is $500 or more and was obtained or purchased by means of a debit instrument that was counterfeit, stolen, etc.
- In a transaction affecting interstate or foreign commerce, furnishing anything of value through the use of a counterfeit, stolen, etc., debit instrument knowing that it is counterfeit, stolen, etc.

b. The Federal Privacy Act of 1974

The Privacy Act of 1974 is codified in 5 U.S.C. Sect. 552a. The criminal penalties for violation of its provisions are contained in Subsection (i)(1)-(3). These criminal penalties may be invoked when a violation of the act, resulting from an unauthorized and willful disclosure of personal information, is made from a computer data base.

The basic provisions of the act are to protect the privacy of individuals. Therefore, an agency, as defined in 5 U.S.C. Sect. 551(1)and 552(e), is prohibited, with a variety of exceptions, from disclosing any record contained in a system of records to anyone or another agency unless the individual has made a written request or has given prior written consent.

If any officer or employee of an agency, knowing that disclosure of specific material is prohibited either by the act or regulations promulgated thereunder, willfully discloses the material to a person or agency not entitled to it, the officer or employee has committed a misdemeanor and will be fined not more than $5,000.

The same penalty is applicable to an officer or employee who willfully maintains a system of records, which could include a computer data base, without complying with the notice requirements of Subsection(e)(4). Subsection (e)(4) requires each agency that maintains a system of records to publish in the *Federal Register* not less than once a year a notice of the existence and character of the record system. The notice must include the system's name and location, the categories of individuals, records and their sources included, the routine use of the records, the system's storage, retrieval, access control and disposal policies and practices, the responsible agency official, procedures used to notify individuals, at their request, that records are contained regarding that individual and procedures for an individual to gain access to the records and to contest the contents of the records.

Finally, the same criminal penalties are applicable to anyone who knowingly and willfully requests or obtains under false pretenses a record regarding an individual.

7. Federal Criminal Code Provisions

At least 40 sections of Title 18 of the United States Code bear directly or indirectly on computer abuse. For ease of analysis, these are grouped into seven broad categories: theft and related offenses; abuse of federal channels of communication; national security offenses; trespass and burglary; deceptive practices; property damage; and miscellaneous.

a. Theft and Related Offenses

18 U.S.C. Sect. 641 (Embezzlement or Theft of Public Money, Property, or Records)—The basic statute that protects federal property from theft is 18 U.S.C. Sect. 641. The statute covers both the thief and the receiver of stolen property. Although most of the terms of the statute are straightforward, several bear directly on computer abuse because of their expansive meanings.

One who "knowingly converts" public property violates Sect. 641. It is no defense to a charge of unlawful conversion that one intended to return the property [cf. *Morissette* vs. *United States*, 342 U.S. 246(1952)]. "[C]conversion...may be consummated without any intent to keep..." 342 at 271-272, or make restitution, unless those acts negate the requisite mens rea. While no court has ever considered whether one may "embezzle," "steal," or "purloin" programs by unprivileged copying or otherwise, it is highly likely that any unprivileged abuse may be styled a "conversion."

> Conversion, however, may be consummated without any intent to keep and without any wrongful taking, where the initial possession by the converter was entirely lawful. Conversion may include misuse or abuse of property. It may reach use in an unauthorized manner... It is not difficult to think of intentional and knowing abuses and unauthorized uses of government property that might be knowing conversions but which could not be reached as embezzlement, stealing or purloining. Knowing conversion adds significantly to the range of protection of government property... 342 U.S. at 271-272. See also *United States* vs. *Tijerina*, 407F.2d 349 (1-thCir. 1969), cert. den. 396 U.S. 843 (1969) (deprivation of control of trucks for a period of time an unlawful conversion within Sect. 641).

The notion of "conversion" is as broad as the definition of the resthat is public property. Moreover, the statute itself is broad enough to include theft of labor or services, *Burnett* vs. *United States*, 222F.2d 426 (6th Cir. 1955) (wrongful conversion of services and labor to two army servicemen by army officer), and uses the catchall phrase "any...thing of value..."

The meaning of the phrase "of the United States or of any department or agency thereof" is broader than absolute ownership. An agency of the United States is, among other things, "any corporation in which the United States has a proprietary interest...;" 18 U.S.C. Sect. 6. "Proprietary interest" is broad enough to include any ownership of stock. Cf. *United States* vs. *Anderson*, 45 F. Supp. 943, 946 (S.D. Cal. 1941) (discussing predecessor to Sect. 641). It may be enough if the United States has the power to control the use of the res, *Bernhardt* vs. *United States*, 169 F.2d 983 (6th Cir. 1948) (property under Army control at Army depot protected by Sect. 641), even if the res is in private hands. *United States* vs. *Echevarria*, 262 F. Supp. 373 (D.P.R. 1967)(advances of United States funds paid to university are protected by Sect. 641).

Although there are no cases directly on point, it seems clear that a joint interest, divided or undivided, or an equitable interest, such as a right to use, may be converted. Thus, should the government purchase the right to use certain programs, and those programs be misappropriated, prosecution should be available under Sect. 641. In addition, one case suggests that property in government custody or possession, even if the government has no legal or equitable title thereto, may be the subject of theft. See *United States* vs. *Gardner*,42F. 829 (N.D. N.Y. 1890) (custom booty awaiting foreclosure as ressubject to theft).

It is clear that if programs are being developed for the government, their theft or conversion violates Sect. 641. Moreover, *United States* vs. *Anderson* shows that raw materials may well be included under this clause [45 F. Supp. at 945-949].

In its broadest interpretation, any misappropriation of programs that are subject to some measure of government control, custody, or ownership is a violation of Sect. 641.

At least two decisions have dealt with 18 U.S.C. Sect. 641. *United States* vs. *Digilio*, 538 F.2d 972 (3d Cir. 1976), was a conviction for conspiracy to defraud the United States and to convert to the defendant's own use the records of the United States, particularly photocopies of official files of the FBI. Defendants contended that Sect. 641 was inapplicable because the government was not deprived of the use of the information contained in the records. They contended that the unauthorized copies of government records were not themselves records and that the unauthorized transmission of the information is not proscribed by Sect. 641.

The government had based its argument of Sect. 641 applicability on*United States* vs. *Bottone*, 365 F.2d 389 (2d Cir. 1966) cert. den. 385U.S. 974, 87 S. Ct. 514, 17 L. Ed. 2d 437 (1966), which held that microfilming of scientific processes with the thief's own equipment and asportation of those copies were proscribed as theft of "goods." The court in agreeing with the government's position, noted that, in *Digilio*, there was no memorization of the information nor copying by the use of the thief's own

equipment. One of the criminals actually used government time, equipment, and supplies to make the copies. Finally, the court stressed that a duplicate copy is a record for purposes of the statute and duplicate copies belonging to the government were stolen.

In *United States* vs. *Lambert*, 445 F. Supp. 890 (D. Conn. 1978), a Sect. 641 (larceny) case, the defendants were charged with selling information derived from a computer within the Drug Enforcement Administration, Washington, D.C. The information included the identity of informants and the status of government investigations into illegal drug traffic. Only the information, not the documents containing the information, were transferred. The defendants contended that Sect. 641 was applicable only to tangible items, such as documents embodying the information, not the information itself. However, the court held that the open-ended "thing of value" phrase of the statute evidences an intent to cover a wide variety of conduct.

The court saw no reason to restrict the interpretation of Sect. 641 to its common law origins. It held that Sect. 641 should cover larceny as well as any new situations that may arise under changing modern conditions and not envisioned under the common law. The court agreed with the government that the property involved was highly sensitive and confidential information maintained in computer records and had a value only so long as it remained in the government's exclusive possession. It thus held that the phrase "thing of value" in conjunction with the explicit reference to records in Sect. 641 covers the content of such record.

18 U.S.C. Sect. 659 (Theft of Goods or Chartels Moving as, Which Are Part of, or Which Constitute Interstate Commerce)—Programs may be sent by interstate common carrier. When they are, Sect. 659 protects them from theft, irrespective of ownership. Unlike Sect. 641, Sect. 659 does not seem to proscribe unauthorized copying per se of programs. Although the statute uses "conversion," it is relevant only to the intent of the actor, and not his act, which must be embezzlement, stealing, etc. The most interesting question posed by Sect. 659 concerns theft from interstate commerce.

An excellent discussion of the elements and breadth of what constitute interstate commerce in Sect. 659 is found in *United States* vs. *Astolas*, 487 F.2d 275 (2d Cir. 1973). In rejecting appellant-defendants' claim that the trucks they hijacked were not yet, or had ceased to be, part of interstate commerce, Judge Medina quoted with approval the trial court's instruction:

> The interstate character of a shipment commences at the time the property is segregated for interstate commerce and comes into possession of those who are assisting its course in interstate transportation and continues until the property arrives at its destination and is there delivered either by actual unloading or by being placed to be unloaded [487 F.2dat 278].

The requirement of the existence of interstate commerce relates to the time of the theft, *United States* vs. *Tyers*, 487 F.2d 828, 830 (2dCir. 1973), so that one who steals a program may not pass it off later to an accomplice leaving the accomplice immune. Nor is it essential that the program ownership be by common carrier to be protected; it is clear that Sect. 659 covers carriage by the owner [*Winer* vs. *United States*, 228 F.2d 944, 947 (6th Cir. 1956), cert. den. 351 U.S. 906(1956)]. It is equally clear that interstate commerce does end sometime, cf. *O'Kelley* vs. *United States*, 116 F.2d 966 (8th Cir. 1941)(theft from boxcar after delivery and partial unloading), but so long as initial steps have been undertaken, cf. *United States* vs. *Sherman*, 171F.2d 619 (2d Cir. 1948) (labeling and delivery of bales of duck canvas to wharf), the program is enroute, cf. *United States* vs. *Maddox*, 394F.2d 297 (4th Cir. 1968) (brief pauses in interstate journey are included within Sect. 659), or yet to be unloaded, Sect. 659 is applicable.

18 U.S.C. Sect. 2314 (Interstate Transportation of Stolen Property)—Unlike Sect. 659, Sect. 2314 apparently requires that the stolen property cross state lines. It does not seem sufficient merely for the stolen property to be introduced into interstate commerce. Although there are no reported cases directly on point, that is, where the stolen property was delivered to an interstate carrier but did not actually cross state lines, statutory analysis in *United States* vs. *Roselli* 432F.2d 879, 891 (9th Cir. 1970), supports this conclusion. In *Roselli*, the court contrasted the anti-racketeering statute, 18 U.S.C. Sect. 1952, with Sect. 2314, noting that use of interstate facilities or participating interstate travel was sufficient to provide jurisdiction for the former, while failing to assert that use of interstate facilities was sufficient to trigger the latter. Moreover, reported cases, involving Sect. 2314, have all involved the crossing of statelines. See, for example, *United States* vs. *Sheridan*, 329 U.S. 379(1946) (causing fraudulent check to cross state lines); *United States* vs. *Hassel*, 341 F.2d 427 (4th Cir. 1965) (causing victim of confidence game to cross state line); *United States* vs. *Jacobs*, 485 F.2d 270 (2nd Cir. 1973) (causing stolen Treasury bills to cross state lines).

The major issue raised by Sect. 2314 is whether a copy of a program stolen, converted, or taken by fraud and transported across state lines can trigger Sect. 2314. The only reported case of a copy used in a related prosecution is *United States* vs. *Lester*, 282 F.2d 750 (3d Cir. 1960), cert. den. 364 U.S. 937 (1961). In *Lester*, a co-conspirator made numerous copies of valuable geophysical maps, and transported the copies across state lines; the appellant was arrested and convicted for conspiring to transport stolen maps in interstate commerce. Rejecting the appellant's

claim that copies were not stolen property, the court held that the property stolen was the valuable idea, not the paper embodiment [282 F.2d at 755].

Although the court in *Lester* found no need to elaborate on its holding, it could have cited *United States* vs. *Handler*, 142 F.2d 351 (2d Cir. 1944), cert. den. 323 U.S. 741 (1944), the most thorough analysis to date of stolen property. After analyzing other case law, the meaning of "stealing," and the legislative history of the National Stolen Property Act, now Sect. 2314, the court in *Handler* concluded:

> (1) the stolen property need not be taken larcenously, that is, there are no requirements of asportation, tangibility, etc.; and (2) the statute is applicable to any taken whereby a person dishonestly obtains goods or securities belonging to another with the intent to deprive the owner of the rights and benefits of ownership [142 F2.d at 353]. Since a copy of a program will indeed deprive the rightful owner of the benefits of ownership, a copying should create the stolen property necessary to trigger Sect. 2314.

Note, however, that in *United States* vs. *Seidlitz*, No. 76-2027 (4thCir. 1978), the trial judge dismissed a count based on Sect. 2314 because what crossed state lines was electronic signals, which he concluded were not property. Seidlitz was convicted of wire fraud.

In re Vericker, 446 F.2d 244 (2d Cir. 1971), was a contempt conviction against a defendant who would not testify before the grand jury even after having been granted transactional immunity. The problem was that the defendant was granted transactional immunity as to Sects. 2314 and 2315 only. The immunity, however, was not applicable to the crimes suggested by questioning of the prosecutor. Sections 2314 and 2315 deal with the theft and receipt of stolen goods, wares, merchandise, securities or money, not FBI documents, which the prosecutor had been interested in. Although the court admitted that in some circumstances mere papers may constitute goods, wares, and merchandise, citing *United States* vs. *Bottone*, 365 F.2d 389 (2d Cir. 1966) cert. den. 385 U.S. 974, 87 S. Ct. 514, 17 L. Ed. 2d 437 (1966), such papers must be well within the normal meaning of goods, wares, or merchandise, that is, property that is ordinarily the subject of commerce. Thus, geophysical maps or secret manufacturing processes are ordinarily the subject of sale and/or license. However, papers showing that individuals are or may have been engaged in criminal activity or what procedures are used by the FBI in tracking them down are ordinarily not bought or sold in commerce, and, therefore, the government did not show that its questions regarding the theft of FBI documents were related to Sects. 2314 and 2315, and, therefore, could supersede the defendant's invocation of the 5th Amendment privilege.

In *United States* vs. *Greenwald*, 479 F.2d 320 (6th Cir. 1973) cert. den. 414 U.S. 854, 94 S. Ct. 154, 38 L. Ed. 2d 104, the Court addressed the issue of whether secret chemical formulae or formulations fall within the statutory language of Sect. 2314 "goods, wares, or merchandise." In *Greenwald*, the number of documents containing the formulations was restricted for purposes of competitive advantage, but one set was given to the defendant, a chemical engineer in the sales department, who appropriated them. The testimony at the trial showed that there was an established market for the chemical formulae and formulation, that is, manufacturers shared formulae by sale or license and treated such as assets similar to machinery or equipment. The court cited *United States* vs. *Bottone*, 365 F.2d 389 (2d Cir. 1966) cert. den. 385 U.S. 974, 87 S. Ct. 514, 17 L. Ed. 2d 437 (1966) and *In re Vericker*, 466 F.2d 244 (2d Cir. 1971), to hold that, given an established, viable, although limited market in chemical formulation, the lawful appropriation of original documents containing such formulations fell within the meaning of Sect. 2314 because the formulations were "goods, wares, or merchandise."

United States vs. *Drebin*, 557 F.2d 1316 (9th Cir. 1977), was a case in which the defendants contended that motion picture photo plays were intangible and could not be considered "goods, wares, or merchandise" under 18 U.S.C. Sect. 2314. The defendants' arguments consisted of claiming that copyrights were intangible property rights, separate and distinct from property rights in the tangible item from which copies are made, and that a copy cannot be acquired by theft, conversion, or fraud because the copyright owner has no proprietary interest in the duplicate of his work. The court rejected these contentions as illogical and contrary to law and held that the copies are goods or merchandise for the purpose of Sect. 2314. Moreover, the court held that the illicit copying of a copyrighted work is no less an offense than if the original were taken.

Finally, in *United States* vs. *Jones*, 414 F. Supp. 964 (D. Maryland 1976), the defendant was charged with transportation in interstate commerce of stolen, converted, or fraudulently obtained securities under 18 U.S.C. Sect. 2314. The defendant claimed that the securities were forgeries and not "securities," noting that Sect. 2314 was not applicable to falsely made, forged, altered, or counterfeited representations of obligations of foreign governments or banks or corporations of foreign governments.

The checks, complete with signatures, were printed by computer as the result of tampering by the employee with the data records stored in the computer. The procedure that the employee used was first to enter an improper vendor code listing, then to enter data regarding the specific checks

to be issued to that false vendor, then to forward to key punch the documents and accounts payable slips, and finally to command from the computer the processing of a check run where the computer would automatically print the checks to the false vendor. The issue before the court was whether these checks constituted forgeries and thus the defendant's conduct inapplicable for punishment under 18 U.S.C. Sect. 2314. The court noted that where falsity in the instrument is in the content, rather than the manner of making the instrument, it is not a forgery. In this case the checks were not lies "in writing," but rather the unauthorized issuance there of. The court held that the mere fact that a computer was used was not relevant because it was simply an inanimate and obedient instrumentality used by the employee similar to a check-writing machine or ballpoint pen and thus was not a forgery.

18 U.S.C. Sect. 661 (Theft within Special Maritime and Territorial Jurisdiction—When programs are stolen in a federal enclave as defined in 18 U.S.C. Sect. 7, a violation of Sect. 661 occurs. As in Sects. 641 and 2314, the question again arises whether unauthorized copying is a violation of the statute. Although it was assumed for analytical purposes earlier that copying is not within the scope of Sect. 661, abroad reading of the statute may well include it. In *United States* vs. *Henry*, 447 F.2d 283 (3d Cir. 1971), the appellant was convicted for stealing a boat within the maritime jurisdiction. On appeal, it was argued that the statute was merely a codification of common law larceny, and since the government failed to offer proof that the appellant intended to permanently deprive the owner of his property, the conviction should be overturned. In rejecting the appellant's claim, the court held that the statute was broader than common law larceny. Drawing on the 2nd Circuit's definition of "to steal" in *Handler*, the court concluded that when one "willfully obtains or retains possession of property belonging to another without the permission or beyond any permission given with the intent to deprive the owner of the benefit of ownership," 447 F.2d at 286, an offense was made out under Sect. 661. As noted earlier, the "deprivation of benefit" theory should enable a prosecutor to support an indictment for unauthorized copying.

b. Miscellaneous Theft and Theft-Related Offense

Although there is no general federal statute prohibiting theft by false pretenses, except 18 U.S.C. Sect. 1025 (false pretenses within the special maritime and territorial jurisdiction) and Sect. 287 (making false claim to United States), courts have construed Sect. 641 to include false pretenses. See *Burnett* vs. *United States*; *Morgan* vs. *United States*, 380 F.2d 686 (9th Cir. 1967) (tax fraud as theft of government money by false pretenses). Thus, there seems no bar to charging one who fraudulently obtains computer usage from the United States, while stealing programs, with a violation of Sect. 641.

Many theft statutes, such as Sects. 641, 659, and 2314, have receiving stolen property provisions as well. In addition, Sect. 662 prohibits receiving stolen property within the special maritime and territorial jurisdiction. Section 2315 proscribes the receipt of goods stolen from interstate commerce. Thus, one who induces the theft of programs not only may be charged as a principal, 18 U.S.C. Sect. 2, or as a conspirator, 18 U.S.C. Sect. 371, but also may run a foul of the foregoing sections.

Numerous federal statutes are designed to cover specific types of theft, but they may be applicable to certain instances of program abuse. For instance, if one has the misfortune to steal a program used in the payment of government money, he violates Sect. 285 that deals with taking or using papers relating to claims. If a government employee wrongfully converts, cf. *Morissette* vs. *United States*, the property of another that is entrusted to him, he commits an offense under 18 U.S.C. Sect. 654. This section would be particularly effective when the employee provided a copy to an unauthorized third party. Theft of programs from federally insured banks and financial institutions is covered by 18 U.S.C. Sects. 655-657, although there is some doubt as to whether nonmonetary property is covered by Sect. 656 because the protected res is "moneys, funds, or credits," in contrast to "other property of value," 18 U.S.C. Sect. 657. But this loophole is closed by 18 U.S.C. Sect. 2113(b), which covers the theft of "any property. . .any other thing of value. . ." from a bank or savings institution. And finally, if a thief "steals, purloins, or embezzles" property "used" by the Postal Service, he violates Sect. 1707.

c. Abuse of Federal Channels of Communication

18 U.S.C. Sect. 1341 (Mail Fraud)—The mail fraud statute has two essential elements: (1) one must use the mail for the purpose of executing or attempting to execute, (2) a fraud or a scheme to obtain money or property under false pretenses. The courts have been generous in their definition of what is a fraud. The classic statement on this count was made by Judge Holmes, "[T]he law does not define fraud; it needs no definition; it is as old as falsehood and as versatile as human ingenuity." *Weiss* vs. *United States*, 122 F.2d 675, 681 (5th Cir. 1941), cert. den. 314 U.S. 687 (1941) (construction scope of fraud in predecessor to Sect. 1341. *Weiss* was quoted with approval in *Blachly* vs. *United States*, 380 F.2d665 (5th Cir. 1967) (referral selling plan as fraud) and *United States* vs. *States*, 362 F. Supp. 1293 (E.D. Mo. 1973) (ballot box fraud in primary election as mail fraud), aff'd 488 F.2d 761 (8th Cir. 1973) (see cases cited therein), cert. den. 417 U.S. 909, 417 U.S. 950 (1974).

Thus, the thrust of the various court opinions would include any scheme to copy programs as a scheme to defraud, and any mailing in furtherance of the scheme would trigger the statute. If the thief uses a mailing to defraud a computer center through services, labor, credit,etc., *United States vs. Owens*, 492 F.2d 1100 (5th Cir. 1974) (mailings which led to receipt of goods on credit as mail fraud), or uses the mailing to obtain the program itself, he falls within the scope of Sect. 1341. The prosecutor should always explore Sect. 1341's applicability in any instance of computer abuse. For a prosecutor's opinion of the effectiveness of Sect. 1341 and, in contrast, the ineffectiveness of the Proposed Code, see Givens, *The Proposed New Federal Criminal Code*, 43N.Y. St. B.J. 486, 488-494 (1971) et passim.

d. National Security Offenses

18 U.S.C. Sect. 793 (Gathering, Transmitting, or Losing Defense Information)—This section, and those that follow in this category, is of limited use in software abuse. But, as a general rule, whenever abuse involves classified, restricted, or defense programs, these sections should be inspected for applicability. Section 793 is broad in scope; Subsection (a), the geographical intrusion provision, covers property owned, controlled, or used by contractors of the government when the property is related to or connected with national defense. The section also proscribes copying of defense information, unlawful reception, communication of contents, and grossly negligent losses. This statute has been held sufficiently definite to satisfy due process requirements, *Gorin* vs. *United States*, 312 U.S. 19 (1941), and has been held to encompass "related activities of national defense" as well as military enclaves [312 U.S. at 28]. See also *United States* vs. *Drummond*, 354 F.2d 132, 151 (2d Cir. 1956) (upholding jury charge in same language).

18 U.S.C. Sect. 794 (Gathering or Delivering Defense Information to Aid Foreign Government)—This statute provides more severe penalties for actual transmission of the defense information to a foreign government and also includes a conspiracy count. One caveat should be mentioned in this discussion of Sects. 793 or 794, or companion statute Sect. 798,which deals with disclosure of classified information. Although public information has always been outside the scope of the protected res [see *Gorin* vs. *United States*; see also *United States* vs. *Heine*, 151 F.2d 813(2d Cir. 1945) (officially disseminated information, no matter how painstakingly culled and digested, is not "defense information")], the Pentagon Papers case, *New York Times Co.* vs. *United States*, 403 U.S. 713(1971), now makes it clear that mere classification is not enough. The flavor of the Black, Douglas, Brennan, and Marshall opinions is that, even in criminal prosecutions, lack of substantial injury to national security might be a valid defense. Even though it is true that Whiteand Stewart contrasted civil injunctive (unpermitted) and criminal (permitted) sanctions, there is language in the Stewart opinion that hints at a need for narrowly construed guidelines on classification. Thus, a clear majority in the case would seem to support the proposition that classified material that had no business being classified, such as information related to Department of Defense lobbying efforts, could not support a prosecution under Chapter 37 of Title 18.

18 U.S.C. Sect. 795 (Photographing and Sketching Defense Installations)—In 1950, President Truman declared pursuant to Sect. 795that all military and commercial defense establishments were to be protected against unauthorized photographing and sketching [Exec. Order10104, 15 Fed. Reg. 597, 598 (February 1, 1950)]. Since the statute covers "graphical representations" of classified "equipment," it is probable that copying classified programs would fall within this section.

18 U.S.C. Sects. 797, 798, 799, and 952—Section 797 deals with subsequent publication and sale of photographs or sketches of equipment denominated in Sect. 795. Section 798, which deals with codes and cryptographic systems, would be pertinent to any abuse at agencies involved in communications work. Section 799 deals with security violations of NASA regulations, and Sect. 952 deals with disclosure of diplomatic codes.

e. Trespass and Burglary

Criminal Trespass—There is no general federal statute covering criminal trespass. In fact, the only statute that denominates trespass a crime in Title 18 is Sect. 2152, dealing with trespass on fortifications or harbor-defense areas. Section 2278(a) of Title 42forbids trespass on installations of the Atomic Energy Commission (ERDA). Neither is particularly applicable to trespass for the purpose of misappropriating programs, unless the situs of the trespass is a fortification, harbor-defense area, or DoD installation.

Burglary—The federal burglary statutes are slightly more comprehensive, but not much. Title 18 provides criminal penalties for burglary of a bank [18 U.S.C. Sect. 2113(a)], post offices [18 U.S.C. Sect. 2115], and interstate carrier facilities [18 U.S.C. Sect. 2117].

(a) 18 U.S.C. Sect. 2113(a) (burglary of a bank). Although some states have denominated copying of trade secrets as larceny, it seems doubtful that entry of a bank to copy programs would make out a federal crime, notwithstanding the language "or any larceny" of Sect. 2113(a). *United States* vs. *Rogers*, 289 F.2d433, 437 (4th Cir. 1961) (the language of the statute refers only to common law larceny). The U.S. Supreme Court has rejected a claim that federal criminal law in this case turns on state law [*Jerome* vs. *United States*, 318 101, 106

(1943) (state felonies irrelevant)]. Once beyond those restrictions, however,the statute is effective against the most traditional defenses. Privileged entry is no defense; see *Audett* vs. *United States*,132 F.2d 528, 529 (8th Cir. 1942) (entry may include "walking in [with] a stream of customers through the front door. . . in business hours"), nor is breaking an element of the offense. Although burglary statutes were originally designed to protect occupied spaces from crime, occupancy is irrelevant for purposes of Sect. 2113(a) [*United States* vs. *Poindexter*, 293 F.2d 329(6th Cir. 1961) cert. den. 368 U.S. 961 (1962)].

(b) Unlike Sect. 2113(a), 18 U.S.C. Sect. 2115 (burglary of post offices) requires forcible breaking as an element of the offense. The only vague term in the statute is "depredation." While the parameters of the term are hazy, depredation is generally held to mean plundering, robbing, or pillaging. See *Deal* vs. *United States*, 274 U.S. 277, 283 (1927) (construing similar language in postal regulations).

Similar to Sect. 2115, 18 U.S.C. Sect. 2117 (burglary of interstate carrier facilities) also requires a breaking. Again, mens rea is intent to commit larceny, which would be common law larceny.

f. Deceptive Practices

18 U.S.C. Sect. 912 (Obtaining Thing of Value by Impersonating an Officer or Employee of the United States)—It may often be the case that one who misappropriates software within a federally protected sphere has falsely represented himself as a government officer or employee in order to gain access to the program. There is no requirement that the "thing of value" be tangible, cf. *United States* vs. *Lepowitch*, 318 U.S. 702(1943) (fraudulent acquisition of information about whereabouts of another), and a copy of the program would certainly seem to fall within the definition. The statute must be read broadly to encompass new concepts of "thing of value" for "it was not possible for Congress in enacting the statute to anticipate all devices and schemes which human knavery might conceive in security benefits. . ." *United States* vs. *Ballard*, 118 F. 757 (D.Mo. 1902) (meals and lodging are a thing of value).

18 U.S.C. Sect. 1001—When Sect. 1001, the catchall that deals with all manner of false representations, is compared with Sect. 912, it becomes apparent that the general rule statute carries a much more severe penalty than the specific statute. In addition, Sect. 1001 requires no fraudulent obtaining of a thing of value; a false,fictitious or fraudulent statement, knowingly and willfully made, is enough to trigger the statute. Whatever one may say about the jurisprudential wisdom of the statute, it seems applicable to almost every instance of computer abuse in the federal sphere. For example, programs may not be divulged to unauthorized persons [5 U.S.C. Sect. 552(b)(4) (trade secrets subsection of Freedom of Information Act)].

Therefore, one who fails to identify himself as unauthorized conceals a material fact, whether or not he represents himself as unauthorized. Is active misrepresentation a less serious crime? Moreover, this section applies to both oral and written misrepresentations. See *United States* vs. *Zavala*, 139 F.2d; 830 (2d Cir. 1944) (false oral and written customs declaration). It may even be applicable to electronic signals from a remote terminal that falsely represent the sender as one authorized to protected software.

18 U.S.C. Sects. 1005, 1006 (False Entries in Records of Banks and Credit Institutions)—Whenever anyone makes a false entry in a bank or credit institution record, with intent to injure or defraud, he runs afoul of Sects. 1005 or 1006. Although both of the statutes are quite fact-specific, they are comprehensive in their respective areas. Since the purpose of the statutes was to ensure correctness of bank records, *United States* vs. *Giles*, 300 U.S. 41, 48 (1937) (teller's failure to file deposit slips is equivalent to the making of a false entry), active or passive omissions or commissions are covered.

Considering the purpose noted above, that is, to ensure correctness of bank records, the breadth with which "bank books" has been interpreted, cf. *Lewis* vs. *United States*, 22 F.2d 760 (8th Cir. 1927) (minutes of meetings of board of directors were "bank books"), and the need to protect banks from loss, *Weir* vs. *United States*, 92 D.2d 634(7th Cir. 1937), it seems reasonable that computer records should be within the scope of Sects. 1005 and 1006. Thus, any false entry, obliteration, or alteration of computerized bank records would be a violation of either Sects. 1005 or 1006.

g. Property Damage

18 U.S.C. Sect. 81 (Arson within Special Maritime and Territorial Jurisdiction)—Although arson may be only infrequently used as a tactic in computer abuse, the prosecutor should be aware of the scope of the statute. A key question is whether hardware or programs may be included within the phrase "machinery or building materials or supplies." A case arising from the Wounded Knee occupation indicates that the definitionof the phrase may be narrowly construed. In *United States* vs. *Banks*,368 F. Supp. 1245 (D.S.D. 1973), the defendant-appellant was accused and convicted of violating Sect. 81 by burning motor vehicles within a federal enclave. Holding that motor vehicles were not "machinery" within Sect. 81, the court through Judge Nichols, invoked *ejusdem generis* and noted the broad interpretation of "machinery" would endanger the statute as too vague, lacking the "requirement of

definiteness . . . that a person of ordinary intelligence must be given fair notice that his contemplated conduct is forbidden . . . " [368 F. Supp. at248]. Thus, a prosecutor might be advised to style any indictment alleging the burning of hardware or software as, alternatively, an attempt to set fire to a building or structure.

18 U.S.C. Sect. 1361 (Malicious Injury to Government Property)—Several cases construing Sect. 1361 demonstrate the liberality with which various courts have accepted indictments charging injury in cases of malicious mischief. Section 1361 was somewhat of a dead letter until interference with the Selective Service began to mushroom in the 1960s. It was resurrected as a catchall to encompass otherwise unindictable offenses. For instance, in *United States* vs. *Eberhardt*, 417 F.2d 1009(4th Cir. 1969), the 4th Circuit considered the famous Baltimore blood-pouring case. Father Philip Berrigan and two others were convicted of violating Sect. 1361 in that they poured blood on Selective Service records. In affirming the convictions, the court utilized the cost of restoring the records as the measure of damages. The appellants did not argue that blood pouring was not "injury" within the meaning of the statute. As a result, the breadth of the case is not clear. At its narrowest, it would mean that any temporary physical obliteration, subsequently restored, is an "injury." While the res in most Selective Service cases was government records at least arguably critical to national defense, other cases construing Sect. 1361 show that neither the injury, nor the res injured need be terribly major. See, for example, *Tillman* vs. *United States*, 406 F.2d 930 (5th Cir. 1969) (glassdoor at induction station broken by draft resistors); *Edwards* vs. *United States*, 360 F.2d 732 (8th Cir. 1966) (plumbing fixture from vacant home); *Brunette* vs. *United States*, 378 F.2d 18 (9th Cir. 1967) (dented fender). Putting all of the cases dealing with Sect. 1361 together with the broadest interpretation of *Eberhardt* may enable a prosecutor to argue successfully that an interference with the use of government software is "injury," and the measure of damage is either the cost of restoration or the cost of development when not restorable.

18 U.S.C. Sect. 1363 (Malicious Injury within the Special Maritime and Territorial Jurisdiction)—This section differs from Sect. 81 only in its substitution of malicious mischief for arson.

18 U.S.C. #2071 (Concealment, Removal, or Mutilation of Public Records)—Another statute that was resurrected during the Vietnam-protest era, Sect. 2071 should be effective against misappropriation of computerized government records, especially when a traditional larceny charge cannot be sustained, for example, copying via a remote terminal without subsequent asportation. The bulk of Sect. 2071 cases deal with Selective Service records and documents; see, for example, *United States* vs. *Chase*, 309 F. Supp. 420 (n.D.I11. 1970); *Chase* vs. *United States* 468 F.2d 141 (7th Cir. 1972); *United States* vs. *Donner*, 497 F.2d 184 (6th Cir. 1974); *United States* vs. *Eberhart*, and thus it would be extending case law to include computerized records as a "document or other thing." Such an extension is rational. The purpose of Sect. 2071 "is to prevent any conduct which deprives the Government of the use of its documents, be it by concealing, destruction, or removal" [*United States* vs. *Rosner*, 352 F. Supp. 915, 919 (S.D.N.Y. 1972)]. The res protected by Sect. 2071 is not merely documentary or written records, but any type of public record. Cf. *United States* vs. *DeGroat*, 30 F. 764(E.D. Mich. 1887) (emphasizing the thrust of the statute as toward records, not papers). And under the rationale of *United States* vs. *Rosner*, dumping or obliterating a computerized record surely deprives the government of its use as much as a blood-pouring, *United States* vs. *Eberhart*, a burning, *United States* vs. *Chase*, or a mutilation, *United States* vs. *Donner*.

Destruction of Property Affecting National Security—The extreme breadth of what constitutes the protected res in 18 U.S.C. Sect. 2153 (willful injury to war or national defense material during war or national emergency) can be seen in its definition in Sect. 2151. War material includes "all articles, parts or ingredients intended for, adopted to, or suitable for . . . the conduct of war or defense activities." Since the mind has trouble visualizing what in the computer industry would not fall within the definition, it seems clear, so long as scienter is proved, hardware and software within the "defense" orbit are protected. Although the statute applies during war or national emergency, the national emergency declared by President Truman in 1950, Proc. 2912, 15 Fed. Reg. 9029 (December 16, 1950), apparently still exists [*United States* vs. *Achtenberg*, 459 F.2d 91 (8th Cir. 1972), cert. den. 409 U.S. 932 (1972)].

The only substantial differences from Sect. 2163 is the applicability of 18 U.S.C. Sect. 2155 (willful injury to national defense material), irrespective of war or national emergency.

Although Sect. 1361 may be construed to reach certain interferences with use, at present there is no provision generally applicable to interference with use or "tampering."

h. Miscellaneous Provisions

Derivative Crimes and Conspiracy—This section covers federal law applications to derivative crimes and conspiracy.

(a) Acts that become criminal only because of the criminal acts of another, derivative crimes, are covered in 18 U.S.C. Sect. 2 dealing with aiding and abetting and Sect. 3 dealing with accessorial liability. As a general rule, any action prior to the

crime that induces the criminal act exposes the one who induced to punishment as a principal. Any action subsequent to the crime in the nature of assistance exposes the assistant to a charge of accessory after the fact. Thus, a third party who induces a theft of software, while not indictable by Sect. 641, is indictable under Sect. 2.

(b) 18 U.S.C. Sect. 371 (conspiracy). Although no general statute makes it a crime to defraud the government, it is a crime for two or more persons to conspire to commit any offense or defraud the United States. This leads to an anomaly—the planning of an act, not criminal in itself, may be a crime. The implications for software abuse are enormous. The broad scope of what it means to "defraud" the United States can be seen in the leading case in this area, *Haas* vs. *Henkel*, 216 U.S. 462 (1910). In *Haas*, three persons, one of whom was a statistician with the Department of Agriculture, conspired to falsify official reports concerning cotton crops and to divulge confidential information concerning those crops to unauthorized persons in order that they might speculate in the cotton market. While there was no allegation of pecuniary loss to the government, the Court rejected a motion to quash the indictment in a habeas corpus proceeding, holding:

[I]t is not essential that such a conspiracy shall contemplate a financial loss or that one shall result. The statute is broad enough in its terms to include any conspiracy for the purpose of impairing, obstructing or defeating the lawful function of any department of Government. . . [I]t must follow that any conspiracy which is calculated to obstruct or impair its efficiency and destroy the value of its operations. . . would be to defraud the United States by depriving it of its lawful right and duty of promulgating or diffusing the information. . . " [216U.S. at 479-480. Accord, *United States* vs. *Johnson*, 383 U.S. 169, 172 (1966) (conspiracy by two congressmen to influence the Justice Department)].

A minor and somewhat redundant conspiracy statute, in the light of the gloss *Haas* puts on Sect. 371, is 18 U.S.C. Sect. 286 dealing with a conspiracy to defraud by payment or allowance of false claims.

18 U.S.C. Sect. 1905 (Disclosure of Confidential Information)—This section is potentially applicable to computer abuse in two types of situations: (a) Where a government officer or employee discloses or communicates the contents of programs in government custody but owned by a private person; and (b) same as (a), but where the government owns the programs.

(a) Obviously, the trade secrets of Sect. 1905, makes the disclosure of "custodial" programs an act illegal unless the disclosure is "authorized by law." For purposes of Sect. 1975, a trade secret is "...an unpatented, secret, commercially valuable plan, appliance, formula or process, which is used for the making, preparing, compounding, treating, or processing of articles or materials which are trade commodities." *United States ex. rel. Norwegian Nitrogen Products Co.* vs. *United States Tariff Commission*, 51 App. D.C. 366, 6 F.2d 491, 495 (1922), rev'd on other grounds, 274 U.S. 106 (1927). See also *Consumers Union of U.S. Inc.* vs. *Veterans Administration*, 301 F. Supp. 796 (S.D.N.Y. 1969) (raw data compiled by government agency not a trade secret of companies providing data). The only law presently requiring wholesale disclosure of information is the Freedom of Information Act, 5 U.S.C. Sect. 552, 871 Stat. 56 (1967); however, it does not apply to disclosure of matters which are trade secrets [5 U.S.C. Sect. 552(b)(4)].

(b) Disclosure of government computer programs. It appears that if the government develops its own programs, such programs must be divulged on demand unless they are classified, 5 U.S.C. Sect. 552(b)(1), or a trade secret. In reality, agencies have been loath to divulge their staff-prepared programs. See, Comment, Public Access to Government-Held Computer Information, 68 N.W. U.L. Rev. 433, 452 (1973). Whether this reluctance is enough to make them trade secrets is doubtful. See *Shapiro* vs. *S.E.C.*, 399 F. Supp. 467 (D.D.C. 1972) (staff-prepared report on off-board stock trading not "trade secret" within 15 U.S.C. Sect. 552 and not prevented from disclosure by 18 U.S.C. Sect. 1905). Indeed, under the definition in *United States ex. rel. Norwegian Nitrogen Products Co.* vs. *United States Tariff Commission*, it seems hard to imagine the government having its own "trade secret," unless it is engaged in a marketing operation. Thus, it seems that any disclosure made pursuant to a 15 U.S.C. Sect. 552 request would exempt the actor from Sect. 1905 liability.

SECTION VII: Overview of Computer and Communications Technology

This section summarizes some of the technical aspects of data processing; it describes basic concepts for investigators, prosecutors, and other law enforcement officials unfamiliar with computer technology and provides a brief review for those more familiar with the technology. After the fundamental aspects of computing—data and programs—are introduced, the computer system structures and modes of operation most commonly found in today's commercial data processing organizations are briefly described. The subject of data communications and networks is then covered separately, as this rapidly growing and changing field of computer technology is so important today. Finally, technical trends and capabilities related to computer and information security are addressed. The glossary and this section of the manual can be used as a convenient reference for technical terms and concepts discussed elsewhere.

Prosecutors and investigators will probably seldom encounter cases requiring the detailed information presented here. If they do have such cases, expert assistance should be obtained; however, understanding the technical concepts in this section will help investigators and others to deal with the experts and handle the technical aspects of the case. Such knowledge will also prepare prosecutors for the possibility of the defense introducting technical concepts during a trial.

Since the introduction of the first computers during the latter years of World War II, computer technology has progressed at an astounding rate. The ENIAC mentioned in Section IV was an early example of electronic technology—a computer of sorts—used to solve computational problems. The IBM Mark I, first used in 1944, was one of the earliest true electronic computers. Whereas the Mark I could perform additions and subtractions of 23-digit numbers in 0.3 second and could multiply 23-digit numbers in about 6 seconds, today's fastest machines perform millions (and in some special-purpose computers, billions) of such calculations per second. More important, today's computers are smaller, more reliable, and less costly than earlier computers. Consequently, computers are found in almost every aspect of our day-to-day lives. In addition to use in government, business, education, medicine, engineering, agriculture, scientific research, and communications, computers are now found in the home, in automobiles, and in many other areas of personal use. Indeed, perhaps no other invention has had such a profound and rapidly pervasive effect on society in such a short time.

The information about computers presented in this section is primarily oriented toward the mid-sized minicomputers and larger mainframe computers typically used for business and commercial data processing. This focus was chosen because investigators dealing with computer crimes will most likely have to deal with this environment. Microcomputers, or personal computers as they are more commonly known, are not addressed in depth in this section of the manual.

In general, however, the concepts applicable to large computers can be scaled down to the personal computer environment. Both require data and programs; the same programming languages exist in both worlds; the basic hardware required for operation—a central processing unit (CPU), memory, disks—is similar regardless of size. The major difference is the number of users each supports. With minor exceptions, a personal computer is a single-user system; minicomputers can support dozens of users and the largest mainframes, thousands of users.

A. Essential Elements of a Computer

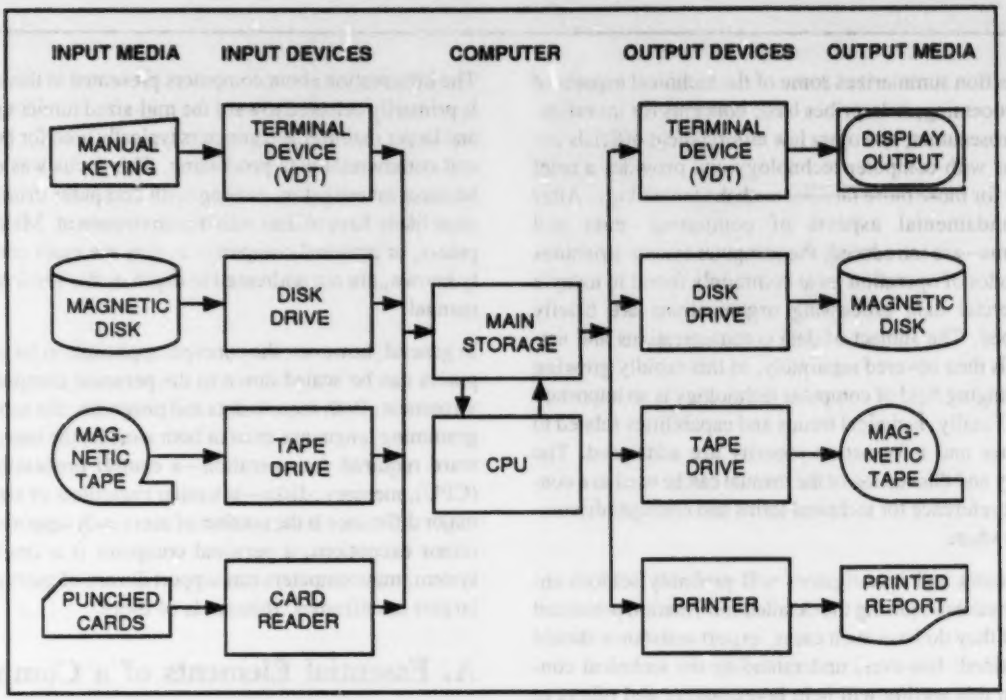
A computer needs two essential elements to process information: the data to be processed, and the program, or set of instructions, that the computer executes to process the data. Computer output is the processed data that result when the input data and program have been properly assembled and the computer equipment has performed correctly.

After a program has been stored in the computer, data are fed through an input device to computer storage (alternatively referred to as main storage). The CPU controls the input and manipulates data according to the program instructions; the processed data, or output, are delivered from the desired computer output device(s). Figure 3 illustrates how data flow from the input media, through the input device in the computer, and through the output devices onto the output media.

The processing performed by the computer is usually of two types: arithmetic processing and symbol manipulation. The difference is basically in the type of data that are processed. Arithmetic or numeric processing uses equations in the form of a program and values supplied by input data for the variables in the equations. The computer determines the answer by adding, subtracting, multiplying, and dividing according to the formula coded in the program.

Figure 3

DATA HIERARCHY



Symbol manipulation by a computer usually involves alphanumeric characters (both letters and numbers) or strings of such characters. An example of symbol manipulation is to arrange, or sort, a list of randomly ordered names into alphabetical order. To do this, the computer needs a different type of program from the one used to process arithmetic values because a different type of input is used and a different output is wanted.

Computers do only what they are instructed to do; they must follow a program, whether processing numeric or symbolic data. Accordingly, programming languages have been developed to provide the communications link between the human and the machine. Hundreds of programming languages are currently in common use today. These range from languages with instructions very similar to native machine instructions, to very high level languages that approach natural language in their usage.

Two of the most frequently used high-level languages are FORTRAN and COBOL. FORTRAN is a language designed for scientific and engineering applications. Its acronym derives from "FORmula TRANslation," reflecting the fact that most FORTRAN programs are used to represent formulas of one kind or another. COBOL, an acronym for "COmmon Business-Oriented Language," is more appropriate for commercial and business applications such as banking, payroll, order entry processing, bookkeeping, and accounting. No hard and fast rules exist, however; scientific and engineering programs can be written in COBOL, and business applications can be written in FORTRAN. Nevertheless, each of these languages was designed to address the requirements of certain sets of problems and thus provides special facilities for that problem set.

Other popular languages include the simple, all-purpose BASIC used in microcomputers; the sophisticated language ADA, the standard of the U.S. Department of Defense; and "C", which is popular for writing computer operating system programs. Programming languages are treated in further detail later in this section.

1. Data

Because computers are used to solve problems posed by humans, they must be able to use the same data that humans use in defining their problems—numbers, letters, words, phrases, and the relationships that tie them together. However, a computer is basically only an electronic machine and responds only to electronic signals. A rather simple hierarchical structure has evolved over the last four

decades of computer use to allow more and more complex types of data and data relationships to be represented and processed by computers.

a. Bits, Bytes, and Words

The simplest and lowest level data element, common to all computers, is the binary digit, or "bit." A bit can have but two values, 0 or 1, and thus is easily represented electronically by the presence or absence of an electric field. (Although the physical implementation of a bit in a computer has changed dramatically over time, from vacuum tubes to magnetic core storage to transistors, the basic concept is the same.)

Increasingly larger combinations of single bits are used to represent all types of data. For example, two bits can represent up to four things, since the 2-bit combination can only have four states—00, 01, 10, and 11. These four 2-bit combinations could stand for the numbers 0, 1, 2, and 3, since that is their value in the base two, or binary, number system, or they could be used as codes to represent the letters J, K, L, and M. Similarly, three bits can have eight states or values, four bits, 16, and so on.

The next commonly defined level above the bit in the computer data hierarchy is the 8-bit "byte," which can have 2^8, or 256 values. A byte can uniquely represent all single text characters commonly used for communication in the English language, including upper and lower case letters, special characters (e.g., #, $, /, +), and the numbers 0 through 9. The term character is often used synonomously with byte. Earlier generations of computers used 6-bit combinations to represent characters, but this limited the available letters to upper case only. Most computers now use the 8-bit convention, but other variations of character size may still be found.

The set of 256 values definable by a byte is called the "character set" of the computer because it contains all available characters. Two standard 8-bit characters sets are used by practically all computer manufacturers—EBCDIC (Extended Binary Coded Decimal InterChange) and ASCII (American Standard Code for Information Interchange). (As with many computer acronyms, these are pronounceable: EBCDIC is "ib-suh-dik"; ASCII is "as-key.")

EBCDIC was developed by IBM as the character set of the System 360 family of mainframe computers first introduced in the early 1960s. It has been used in all architectural successors to the 360 series and by a few other computer manufacturers as well. EBCDIC is considered a de facto standard because of the comparatively large number of IBM mainframes installed throughout the world.

ASCII is a true international standard, developed and sponsored by the American National Standards Institute. It is the character set used by most of the rest of the world's computer manufacturers and by IBM for some of its computers other than the 360 family. Although ASCII is an 8-bit character set, only the first 128 values are currently defined.

Text data are typically stored in a computer as a string of contiguous bytes, each byte representing a single character of the text. Thus, the name "John Doe" is stored as a string of 8 bytes (the blank space counts as one character), and the address "123 Main Street" requires 15 bytes.

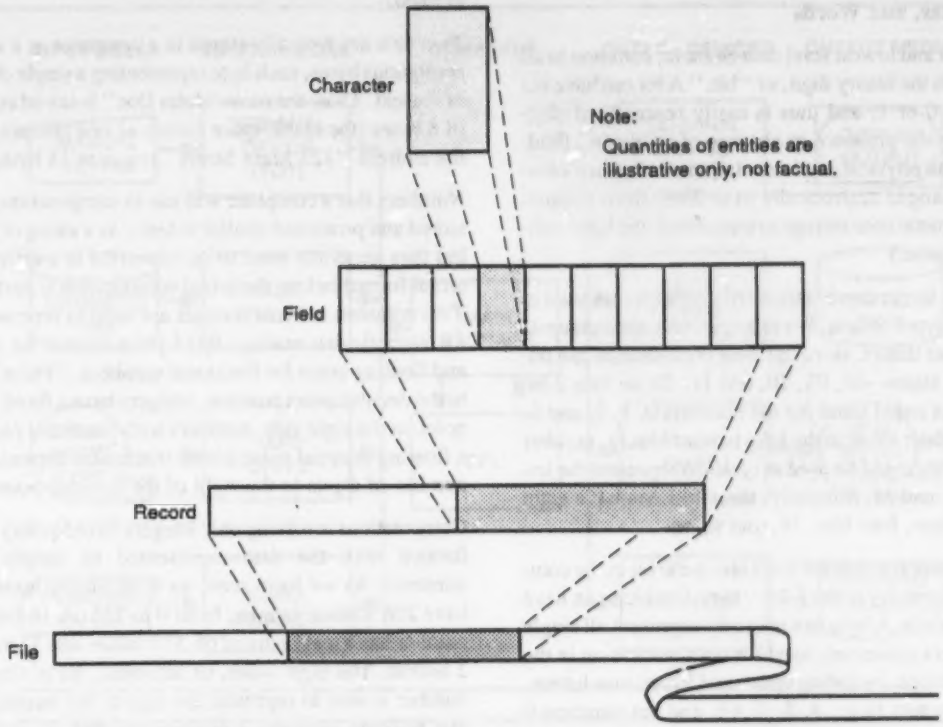
Numbers that a computer will use in computations can be stored and processed similar to text—as a string of bytes—but they generally need to be converted to a different internal format before the actual computation is performed. Two common internal formats are used to represent data for numeric processing—fixed-point format for integers and floating-point for fractional numbers. "Point" refers to the decimal point position. Integers have a fixed decimal point on the right side; numbers with fractional parts have a floating decimal point whose placement depends on the number of digits to the right of the decimal point.

Computations involving only integers (fixed-point) are performed with the data represented as simple binary numbers. As we have seen, an 8-bit binary number can have 256 values, ranging from 0 to 255. A 16-bit binary number has a maximum of 65,535 values and 32 bits, over 2 billion. The high-order, or left-most, bit of the binary number is used to represent the sign of the integer; a 0 in that position indicates a positive number, 1, a negative number. For example, 00000011 equals 3 and 10000011 equals −3 for 8-bit fixed-point numbers. Thus, 16 bits can typically represent the integers from −32,767 to +32,767. All computers have hardware instructions for fixed-point computation.

The representation of a floating-point number is considerably more complex than fixed-point. Although differing from computer to computer, the representation is quite similar to the scientific notation frequently used by engineers, where numbers are expressed in two parts: a fractional part containing the significant digits of the number, and an exponent, or power, to which 10 must be raised to create the actual value. For example, the number 106.54972 can also be written as 0.10654972×10^3; in scientific notation, this is written as 0.10654972E3. (The "E" is a convention of the notation signifying exponent.) Likewise, floating-point numbers in computers also have two parts, a fraction and an exponent. In general, the magnitude of a floating-point number is practically unlimited; the precision, however, is limited by the number of bits used to store the fractional part. Some computers have a "double precision" format in which twice as many bits are used to store the fractional part. Floating-point computation may be done in hardware or software depending on the type of computer.

Figure 4

DATA HIERARCHY



Both fixed- and floating-point numbers are stored in a computer "word," the next level in the data hierarchy. The size of the word depends on the architecture selected by the manufacturer. Microcomputers typically have 16-bit words, but 8-bit and 32-bit microcomputer words are not uncommon. Most popular minicomputers and mainframes have 32-bit words; however, 36-bit and 64-bit words have also been used by major manufacturers. Text is also stored in words, with the number of 8-bit characters per word dependent on word size. Four characters per word is the most common implementation. The computer word is also the basic addressing unit of computer memory, although some computers have memory addressable at the individual byte level.

b. Fields, Records, and Files

The levels of the data hierarchy discussed above are basically physical in nature—that is, they depend on the physical nature of the implementation of the computer architecture, the manner in which data are represented and stored in memory or on a storage device. From this point on, the data levels that will be addressed are logical. They do not depend on the computer, but on the nature of the data itself. "Logical" is the word often used to refer to the way the user or programmer views the data.

Data fields, records, and files are logical data levels, although they obviously must be physically stored in the computer. These levels are also called data structures; their relationship to each other and their position in the data hierarchy are shown in Figure 4. Fields consist of a number of contiguous alphanumeric characters with a particular meaning, such as a name or account number. Related fields make a record, and a collection of associated records form a file. (Another common name for a file is data set.)

Fields, records, and files are all named structures in a computer system. The name must be sufficiently unique to allow complete identification of the structure. Within a record, all fields must have unique names; within a file, all record types must have unique names, although most simple files contain only one type of record. Finally, within a computer system, all files or data sets must have unique names.

The data record containing customer information for a billing system provides an example of data structures used in

a computer application. In this example, a data record named the customer-record is maintained for each customer based on sales slips, payment receipts, and other input data (see Table 21). The collection of all such records may be called the customer-file. Typically, every record in a file such as the customer-file contains the same data fields.

c. Data Bases

The highest level in the data hierarchy is the data base. In a generic sense, the term data base may be used to refer to all data used by a department in an organization or by the entire organization. In this context, data base could be literally interpreted to mean all data that exist in the organization, whether computerized or not. In the day-to-day world of commercial data processing, however, data base has a more specialized and common meaning.

Table 21

Makeup of Customer Data Record

Data Field	Data Content	Sample Data
Account	Account number	123 54 6789
Name	Customer name	John Brown
Street	Customer street address	123 Main Street
City	Customer city/state/ZIP	Anytown, CA 94001
Balance	Ending balance, previous month ($)	38.78
Charges	Total of items charged during month ($)	16.50
Payment	Payments on account during month ($)	38.78

A data base is both a collection of the occurrences of different types of named records and the relationships that exist between records, groups of logically associated data items, and individual data items. The important difference between a data base and a file is that a data base contains information about relationships between data as well as the actual data itself. A file merely contains the data; the relationships between files must exist in another place, often in the programs that access the files. Use of data bases, therefore, can simplify the programming task; the relationships need only be defined once in the data base, not many times in all of the using programs.

In the billing example above, the charges field contains the total amount of charges the customer has made during the month. This information may be sufficient for billing purposes, but a customer may, under unusual circumstances, also wish to know details of all individual charges (e.g., date of purchase, store where purchased, individual items and prices). In a computer application based on files, these detailed data would probably be included in the customer record itself, burdening the record with seldom-used data. In a data base application, the customer record need only have a "pointer" to a record in, for example, a separate detail file that contains only the charge detail information for each customer. The pointer defines the relationship between the customer file and the detail file. Many such relationships exist in typical application data bases.

The manner in which data bases are logically and physically constructed and accessed has been a subject of continuing academic and commercial interest for many years. Many claims are made about the benefits of data base usage, including the increased efficiency and productivity of programmers using data bases in application development. The widespread use of data base technology would seem to substantiate these claims. All major computer vendors, as well as a number of third-party software companies, have developed and marketed proprietary data base management systems (DBMSs), system software packages that provide tools that facilitate data base design, implementation, and use. These DBMSs are widely used in on-line transaction systems.

The technical aspects of data base implementation and usage are complex and vary considerably from system to system. Most competing DBMSs are very different; in fact, a single computer manufacturer may offer more than one DBMS, using different implementation technologies to meet differing user requirements. For those interested in further detail concerning data bases, DBMSs, and related technology, several excellent books are available specializing in these topics[37,38].

2. Programs

A computer cannot yet be directly instructed in English or other natural language, but instead responds to specially coded instructions—a computer program. A typical program is a series of instructions or statements that explicitly directs the computer how to manipulate the data to be processed so as to produce a certain result. A program typically contains instructions for reading data, for manipulating data in various ways, for deriving new data from old, and then for storing or writing data. Writing includes the creation of new files (on magnetic tape, disk, or other media) as well as printing.

Computer programs are often referred to as "software" to distinguish them from "hardware," which refers to the computer equipment. A word of caution, however: These terms are jargon; they have variable meanings and should not be used for legal purposes. Software often refers to the

computer program along with its supporting documentation. Program documentation includes specifications, flow charts, input and output (I/O) formats, test input data, sample output data, operating instructions, and program listings. Further confusing the terminology is "firmware," a combination of hardware and software where computing instructions (software) are resident in a special memory device not directly accessible by computer users and are considered to be an integral part of computer circuitry (hardware).

Software is generally divided into two categories—application software and systems software. Application software refers to the programs that are designed and developed to solve the problems of the end users of computers, whether engineers, scientists, or business people. Application software is typically developed by the owner of the computer system, although numerous computer owners purchase commerically developed applications. Most computer software falls into the application category.

System software is the collection of programs necessary to operate, maintain, and support the data processing environment. This category includes the operating system (or system control program), data communications programs such as teleprocessing monitors, DBMSs, programming language translators, and utility programs for system maintenance and administration. System software is usually developed and supplied by the vendor of the computer system and/or specialty third-party developers. In this area, the system owners are typically responsible only for installation of system software computer programs and limited maintenance activities.

a. Program Instructions

In most computers, instructions have two major parts: an operation and an operand or operands. The operation describes what action the CPU is to take—for example, add, subtract, multiply, compare, transfer control, shift, read, or write. The operands identify the memory locations of the data to be processed or the data to be used, depending on the type of command. Many instructions have two operands, a source and a destination.

Figure 5 shows an instruction with the operation "ADD" and an operand "Z." The arbitrarily assigned, binary-coded instruction for ADD is 00001010 and the symbolic address Z for the data to be added is at binary-coded location 10110010. Note that the data to be used, in this case added, is not Z (10110010), but the data stored at the location in the computer memory with the address Z (10110010). Because the results of the addition will be stored in an internal location known as an accumulator, no second operand is required. The codes, although arbitrary here, have meaning to the computer.

In most businesses a computer processor does one and only one thing at a time; that is, a program's instructions are executed one at a time. To make the processor's actions automatic, computers are designed to perform the next instruction in memory following completion of the execution of the current instruction. The next instruction is defined as the instruction beginning at the last memory location of the just-completed instruction plus 1.

Consider, for example, the ADD instruction of Figure 5. If it was the last instruction executed by the processor and it begins at memory address 100, the next instruction to be executed would be at memory location 102. Since the ADD instruction is two bytes in length, its last memory location is 101, and adding one yields memory location 102.

The programmer can override the processor's automatic next instruction assignment at any time. Special instructions known as "transfers" or "branches" provide this capability. The operands of these instructions contain the programmer-specified next instruction location or memory address from which the next instruction is to be obtained for execution. Typically, the computer processor has a built-in counter always containing the memory location of the next instruction to be executed. The transfer or branch operations change this next-instruction counter to the programmer-specified location contained in the operand of the transfer or branch instruction.

To perform data processing, the computer must have access to both the data and the set of instructions that cause it to perform its operations in a specified sequence. Therefore, computer programs contain both the instructions or procedures the computer is to follow and a specification of the data to be processed. There are several types of each, including:

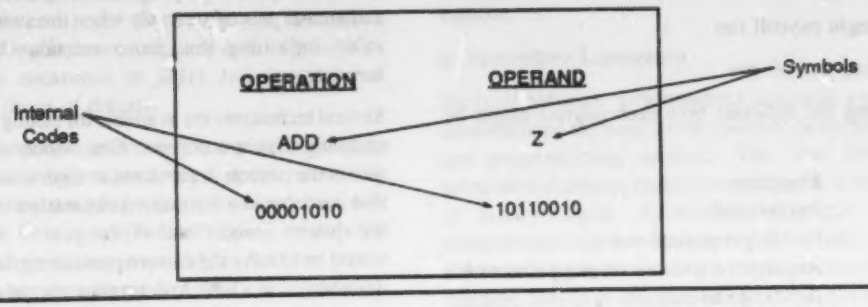
- Instructions or procedures: I/O operations, arithmetic, decision or conditional, editing, logical operations, imperatives, and others.
- Data: file and other definitions, constants, variables, and others.

Input instructions cause data to be moved from connected storage devices such as magnetic disks and tapes, optical disks, and terminal keyboards into a section of the computer's memory area reserved for temporarily storing information that is now being worked on and for saving intermediate results. Output instructions move data from that same temporary or working storage to the connected storage devices, disks, tapes, etc.

Arithmetic instructions perform the fundamental operations of arithmetic—addition, subtraction, multiplication, and division— according to the rules of arithmetic. The

Figure 5

A COMPUTER INSTRUCTION



values used in the calculations are obtained from memory, and the results are usually stored in memory.

Decision or conditional instructions determine the course of action the program is to follow next, based on the results of a test of the conditions then existing. Data in memory may be compared to other memory-resident data or a constant, and the program will follow different courses of action based on the results of the test (e.g., equal to, less than, or greater than conditions).

Editing instructions modify the format of data in memory to prepare for their use in output or in other instructions. Common examples include rounding, suppressing leading zeros, shifting data to the left or right within a field, and insertion of special characters, such as dollar signs and carriage return (CR) signs.

Logical operators are similar to arithmetic operators except that the results of the operation are obtained by combining operands using logical rules. Typical logical operators are AND, OR, and NOT, and combinations thereof. Logical operators and decision/conditional instructions are often combined to test several conditions in one statement.

Imperative instructions specify an unconditional action to the computer. Common imperative instructions are MOVE, where data in one storage location are moved to another storage location specified in the instruction, and GOTO, where the processor proceeds to the memory address specified in the GOTO instruction to determine what instruction to execute next.

Other miscellaneous instructions are available in most computer systems. These perform such operations as testing for end-of-data files, testing equipment readiness, and accessing time clocks built into the computer. The number and function of these instructions vary with the design of the computer.

File definitions describe the content of the records in data files. Each item of data in the record is assigned a beginning and ending location relative to the beginning of the record. Records are often grouped together, or blocked, in a data file and each individual input or output operation will transfer a group of records from or to the file. File definitions often define the number of records in each group.

Constants are defined fixed values or data items that do not change during the operation of the program.

Variables are defined data items whose values can be changed during the operation of the program. Variables are usually initialized to a beginning value at the start of execution of the program. That value is subject to modification by the program during its operation.

Parameters and indexes are types of variables that usually represent information about the processing activity such as the number of times an operation is to be performed.

b. Programming Techniques

Certain techniques have been developed that reduce the level of effort required to design, code, and test or debug programs. The more common techniques are described below.

Loops—Certain sets of instructions are used repeatedly in most programs, whereas other sets are used less often or not at all. A typical payroll system for paying 10,000 people may include the following instruction sets:

- Used for all employees
  - A. Gross pay calculation
  - B. Gross to net calculation
  - C. Prepare earnings register
- Used for nonexempt employees only

D. Verify overtime payments

E. Calculate overtime pay

- Used for each payroll run

F. Begin payroll run

G. End payroll run

The following list indicates how each payroll might be performed:

Program Step	Function Performed
1	F. Begin payroll run
2	Are there any more employee records? If NO, go to step 11.
3	YES, get next employee record
4	Is this employee exempt? If YES, go to step 7.
5	D. Verify overtime payment
6	E. Calculate overtime pay
7	A. Gross pay calculation
8	B. Gross to net calculation
9	C. Prepare earnings register
10	Go to step 2.
11	G. End payroll run

This use of the loop from steps 2 to 10 allows the programmer to save considerable effort by writing each set of instructions only once instead of 10,000 times. In addition, the programmer can use the basic pay calculation in routines A, B, and C whether or not there is overtime. This approach is called looping because the computer will execute from instruction step 2 to 10 and then circle (or loop) back to step 2 until all employee records are processed.

Steps 3 through 10 are used conditionally if the answer to the question in step 3 is YES. This is known as a conditional loop. Frequently, programs will contain what is known as nested loops, where a loop within a loop will be repeated a number of times before the outer loop is completed once.

Tables—Programs frequently use sets of data items stored in memory. The program obtains information from the table by searching the table until it can match the data it is now working with against an entry in the table. For example, the airport code for Chicago is ORD and for Portland PDX. A flight record obtained from a data file could be converted as follows by using three tables:

Input Data	Table Name	Reported Value
ORD	Origin	Chicago, Illinois
PDX	Destination	Portland, Oregon
ORD/PDX	Fare	$750

Program Switches—Often, the results of a conditional test need to be saved for later use in a program. The programmer can accomplish this by setting a variable value that represents the test results. Payroll systems often use a switch to indicate whether this payroll process is the last for the quarter and another to indicate whether it is the last for the full year. The program will perform the quarterly and annual procedures only when the switches contain the value indicating that those calendar milestones have arrived.

Several techniques are available for setting the switches and ensuring they are correct. One widely used method requires the payroll department to enter a transaction record that contains key indicator information, such as "end of the quarter" and "end of the year." Another method would be to have the current processing date tested against dates stored in a table to determine special date-related processing requirements.

Subroutines—A routine is a sequenced subset of instructions that produce a particular result (e.g., a date conversion). These frequently used instructions are segregated into what is known as a subroutine. Subroutines are designed to be used from anywhere in the program and are called on where and as needed. When the operations specified in the subroutine are completed, the program then returns to the main routine. Subroutines may themselves use other subroutines and may even call themselves recursively, depending on the function performed by the subroutine. Subroutines are also important for organizing the structure of a large program to make it more comprehensible.

Program Modularity—Most computer programs or subroutines contain only several hundred statements in their originally coded version. A compiler, or language translator, translates these several hundred statements into a greater number of machine language instructions, typically 500 to 1,000. Typically, one programmer can complete a program of this size in 2 or 3 weeks.

Programs of this size have limited objectives and can be "read" and understood by an individual familiar with the programming language used. However, these programs are nearly always part of a much larger system containing many such programs and subprograms. To fully understand the significance of any one program, a programmer must know what the previous programs did and what the following programs will do. For example, a prior program may alter the data being processed in unexpected ways, or a succeeding program may contain assumptions about the work performed in this program. This interdependency of programs in a large system requires the entire system be analyzed before the role of any single program in the system can be understood.

Some computer programs perform many tasks and may contain many thousands of computer instructions. These programs are usually broken down into discrete sets of instructions with an identifiable purpose. These sets are called modules. Modules contain subroutines or use

subroutines in other modules. An airline reservation system contains many modules. Each program module can be programmed and tested by a different person, and large programs are designed in modular form so that several or many programmers can work on the program simultaneously. Development times and cost for programs of this size are measured in years and hundreds of thousands or millions of dollars.

Predictably, these programs are very complex, and highly qualified programming experts may spend weeks or months to understand one phenomenon such as occasionally erratic results. One reason for developing modularity was to allow a programmer to quickly narrow the possible sources of such phenomena to a likely few modules, thereby eliminating the need to examine the entire program. Typically, programmers spend more of their time finding and correcting errors or bugs in their programs than they spend designing and writing them.

A program or system of programs to perform a major application such as payroll, general ledger accounting, or inventory control is often so complex that unauthorized functions can be hidden in them (converting them into Trojan horse programs). Programs of this size are seldom totally free of errors because there are too many conditions to test on a practical basis.

3. Programming Languages

Programming languages are designed to enable human programmers to communicate more easily with the computer in a language more nearly like their own to cause it to perform specific operations in a defined sequence. These languages must be translated into a form that the computer can understand and execute, namely machine language—a set of hardware-level instructions. Because each vendor's computer model or model series has a different circuitry design, machine languages differ from computer to computer. Higher level languages tend to be standardized for many vendors' computers, however.

Although a program can be written in machine language (by directly coding zeros and ones to represent the binary OFF and ON memory states of the machine) and all early programming was done in this manner, today's programmers use languages that are at least one or more steps removed from this level for developing software. When such a language is used, a language translator program must be executed with the source program as input data to create machine language output data. The source programs translated into machine language form are then said to be in object code and are ready to perform processing. Some translators called interpreters convert source language into object language each time the source language is to be used, one source statement at a time.

The major types of programming languages, in addition to native machine languages, are assembler languages, high-level compiler languages, very high level languages, and specialized languages. A description of each type follows.

a. Assembler Languages

Early experience with machine language programming demonstrated the need for an easier-to-learn and easier-to-use programming method. The first developments substituted character mnemonics (memory aids) for the sets of binary digits. Assembler languages use easily remembered symbols such as "A" for add and "S" for subtract. In general, assembler language instructions match machine language instructions on a one-for-one basis.

Assembler languages also provide symbolic addressing capabilities; that is, memory locations containing variables, constants, or other instructions may be referenced using a symbol rather than the absolute memory address. This capability facilitates assembling programs and storing data at different locations in the computer memory each time the program is assembled and executed. An example is shown below. The add instruction refers to the memory address of the operand to be added by using the symbol FIVE, rather than its binary address.

Symbol	Operation	Operand	Comment
	ADD	FIVE	Add 5 to accumulator
FIVE	CONST	5	Define constant

Programs coded in assembler languages must be processed by a special computer program known as an assembler that translates the assembler language coding of the programs into the machine language coding used by the computer.

b. High-Level Compiler Languages

High-level compiler languages perform the same and more functions than assembler languages do. In contrast to assembler programs where each line in the source code becomes one machine instruction, high-level compiler languages can express the equivalent of many assembler or machine instructions in only one line or statement in source code. This translation is performed using a special computer program known as a compiler. Some compilers translate into assembler code and must use an assembler to achieve machine code.

In addition, compiler languages are designed to match more closely the normal language of people. In an example where one number is doubled and then added to another, the programmer's source code might appear as follows:

	Code	Translation
Assembler	L N/Z	Load N into storage location Z
	M Z/2	Multiply the number at location Z by 2
	A Z/X	Add the number at location Z to the number at location X
FORTRAN	X = X + 2*N (= means replaced by) (* means multiplication)	Let the number at X become X plus twice the number at N
COBOL	ADD NUMBER *(2) TO ANSWER	Add the value of NUMBER times 2 to the number at ANSWER

Note that the programmer's coding in all three languages will convert to either the same machine instructions or their equivalent, and the same result will be obtained.

Many of today's high-level compiler languages are known as machine-independent languages. The design objective is to allow a program written in one of these languages to be used on different types of computers with few, if any, source coding changes required. Each type of computer has a unique compiler that converts the high-level source coding as required by the machine language for that computer. Note, however, that compilers can be written in their own or other high-level compiler languages, which allows languages to be propagated from one type of computer to another.

Most commercial programming is now done with high-level compiler languages, of which the most common are:

COBOL	COmmon Business-Oriented Language
RPG	Report Program Generator
BASIC	Beginners All-purpose Symbol Instruction Code
FORTRAN	FORmula TRANslation
PL/1	Programming Language, version 1
APL	A Programming Language
ADA	Named for Ada Augusta Lovelace

In recent years, a number of high-level compiler languages have been developed in the academic and research communities as teaching and computer science research tools. Several of these have become popular for third-party application and system software development, particularly for micro-and minicomputers. The most widely used of these are "C," developed at Bell Labs for use with the Unix™ operating system, and Pascal and Modula, both originally developed as university teaching and research tools.

d. Very High Level Languages

The high-level compiler languages described above are primarily used by trained professional programmers. A current trend in the data processing industry is for computer users to become more involved in developing their own software. In support of this trend, a number of even higher level programming languages have been developed and marketed specifically for this type of programming. These are generally called "fourth generation languages" or "4GLs" and are typically used in conjunction with a DBMS for extraction and reporting of data.

Some of the features of fourth generation languages include natural language (or very close) syntax, nonprocedural coding (sequence is unimportant), powerful query and menu capabilities, and decision support analysis and business modeling functions. Current popular packages include FOCUS, NOMAD, and RAMIS from third-party software developers. Computer vendors also provide many of these end-user capabilities with their proprietary DBMS packages.

Interestingly, professional programmers also use fourth generation languages for some application development. The primary advantage is increased development productivity; the disadvantage is comparatively greater computer resource usage than with other languages.

e. Specialized Languages

The flexibility of compilers has encouraged the development of many specialized programming languages. One example is APT (automatically programmed tools), a widely used specialized language. The APT compiler converts source code developed by a specially trained programmer into a set of machine tool control instructions. These machine control instructions guide numerically controlled machine tools through the series of operations necessary to perform various steps such as milling and boring.

Other high-level languages exist for systems simulations, report preparation, text editing, typesetting, and so on. Whenever sizable groups of programmers are coding programs to perform specialized functions that can be standardized, the opportunity and incentive exist to develop a specialized language that will improve their productivity. The suppliers who decide to sell computers or computer services to that market provide the necessary compilers to translate the specialized language into the machine language required by their computers.

Computer programs have become very valuable intellectual products, making them costly and of high proprietary value. Therefore, they are often protected by copyright or as trade secrets and are as susceptible as any other valuable work to criminal and abusive intent.

B. Computer System Structure

1. Computing Equipment

The size and capacity of computers generally available today range from programmable pocket calculators that sell for less than $100 and personal computers that sell for a few thousand dollars to large mainframe systems and superhigh-speed machines (supercomputers) that cost many millions of dollars.

Computer systems are generally grouped into four categories according to their size: microcomputers, personal computers, and workstations; minicomputers and mid-range systems; mainframes and other large-scale systems; and computer networks. The dividing lines between the categories are not always clear, however; some workstations are more powerful than some minicomputers, some minis more powerful than certain mainframes, and so on. The following examples illustrate the differences. Computer networks are discussed in a later section on data communications.

A small computer may help to automate some small application (e.g., the accounting and payroll system for a small enterprise) or to design promotional mailings. Machines of this capacity are generally referred to as minicomputers or mid-range systems, although a small "mainframe" may also be used. To further complicate things, a single microcomputer or a network of them might also be used for this purpose.

A computer with several high-speed input and output units and a storage capacity of several hundred thousand characters could support the numerous processing tasks of a large brokerage firm. This computer could be considered a medium-sized system and could be replaced with a large minicomputer or smaller mainframe system.

A large computer system often includes equipment costing millions of dollars, many high-speed input and output devices to handle several types of data, a huge storage capacity of billions of characters sometimes employing hundreds of disk drive units called a disk farm, several processing units handling different jobs at the same time, and perhaps even communicating processors that reside at different locations. Although this system would generally be a mainframe complex, the computing requirements might well be satisfied by a cluster of networked large minicomputers.

Regardless of the size, capacity, and location, the hardware components of any computer system include input and output devices, storage devices for internal and external storage (or auxiliary detachable storage), and the CPU. The functional characteristics of these components are as follows:

- Input devices, which accept data and programs into the system.
- Output devices, which move data from the system, or store instructions or data for recycling input back to the system.
- Storage devices, which store the programs and data to be used by the system.
- Processing and control devices, which execute the programs to perform logic and arithmetic and manipulate and move data within the system.

Several types of input and output devices may be used with a computer system. Some perform only input or output functions. Some perform both input and output; and some have input, output, and storage functions.

A common input device used is the punched card reader. The card reader performs the input function by sensing the holes punched in a card and emitting electrical signals to the computer, based on the position of the holes, to indicate certain characters or numerals. Although punched cards are not used nearly as much for input as they were at one time, they are still in common use and many computer centers still have a card reader attached to the system.

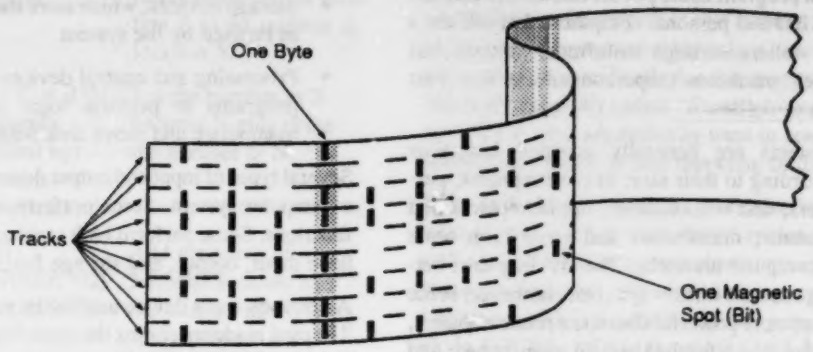
Similar devices are used for key-to-disk or key-to-tape input. An operator at a terminal keys the information through a conversion system directly to disk or tape storage. An alternative is data entry directly from the terminal into the computer system using an on-line application, thereby eliminating the tape or disk reading step from the production processing. In addition, this alternative provides for real-time editing and verification of the input data and usually does not require a second re-entry step for invalid data.

Other types of input devices are optical character recognition (OCR) readers, magnetic ink character recognition (MICR) readers, and point-of-sale (POS) terminals. An embossed charge card, for example, is designed for OCR as are special pencil marks in predetermined positions on a card or paper used for multiple choice examinations. Most banks use MICR to process checks and other documents automatically. Retail establishments use POS terminals to record transactions; a keyboard or sensors (sensing wands) attached to a terminal are used to read data from the tags (Universal Product Code) on the product being sold as well as on the purchaser's credit or debit card.

Output devices include the card punch, tape punch, and printer that are used to transfer data out of the computer into the medium used with each device (e.g., cards, paper tape, paper forms). Another output-only device is the computer-output microfiche or microfilm (COM) recorder. Because the data from the computer are recorded on photosensitive film in microscopic form, data can

Figure 6

DATA STORED ON MAGNETIC TAPE



be printed in more concentrated form than with standard printed output. To be retrieved, however, the data must be read through a microfilm reader.

An example of a device that can be used for both input and output is the control console, a device containing the controls and indicators that allow communication between the computer system and operator. The operator uses the console to start and stop the system, receive instructions and status information, control some of its operations, and insert special instructions or data. Similarly, video display terminals (VDTs) and hardcopy terminals (such as a teletype terminal) provide input to or output from the computer. All of these devices use keyboards to key data into the computer. For the VDT, output from the computer is printed on a video screen or monitor, whereas output provided by a hardcopy terminal is printed on paper. Magnetic tape, disk, diskette, cassette, cartridge, and drum devices may be used both for input and output. As mentioned in Section IV, optical disks are also available but can only be used for input—they are essentially read-only devices.

High-speed storage devices retain data and programs during processing. Other names that are frequently applied to the principal storage unit in a computer system are main storage, central storage, or core storage (although technically obsolete). In most cases, the word "storage" can be readily replaced by "memory" with no change of meaning. Typically, all data pass through main storage on their way to or from the CPU, input and output devices, and auxiliary storage.

Auxiliary, secondary, or peripheral storage in the form of magnetic or optical media expands the storage capacity of a system but has far slower access. Data stored on magnetic media are in the form of tiny invisible magnetized areas that are sensed and written electronically. A magnetized spot represents the binary digit 1, and an unmagnetized spot represents 0. The diagram in Figure 6 illustrates coding of data on a magnetic tape. Storage on other magnetic media is similar. Optical media use a laser beam for sensing data and are similar to compact disks used for music.

The CPU performs the data processing functions that the program directs. It also controls the movement of instructions and data within the system. The CPU usually has two functional sections: a control section and arithmetic-logic section. The control section directs the I/O devices, decodes and executes instructions, and routes data between storage and the registers and arithmetic-logic unit. The arithmetic-logic section contains the circuits that perform arithmetic and logical functions.

The CPU also has one or more sets of registers, high-speed memory areas that are designed to temporarily store data, arithmetic and logical operands, results, and instructions to be processed. For example, registers may be used to hold the address for a particular item of data, to hold a variable or constant data item, to accumulate arithmetic/logical results, and to act as indices into tables of data items.

2. Operating Systems

a. Functions of the Operating System

A computer operating system consists of the programs that manage the computer operation and the connected I/O devices. Operating systems perform such functions as data transfer between the processor's storage and I/O devices, allocate storage space, determine which task will be performed next, keep a record of events, communicate with the computer operators, and often contain the system's

compilers and various programs for general use as well. The tasks are generally performed asynchronously and are queued to be performed when resources become available or when one task depends on another.

The objectives that an operating system must meet for a user's job or run are to: automate the steps in a job-to-job transition and in the setting up of a specific job; accommodate an environment of diverse applications and operating modes; reduce total job time and increase efficiency; provide necessary diagnostic aids; provide security controls for data, program, and user integrity, confidentiality, and availability; and increase programmer productivity.

Typically, an operating system consists of an executive control program and a number of processors. Each processor performs a specific function upon command of a control statement provided by the operator or application program. The function of each processor is job management, data management, or task management. A list of some major operating system functions, according to type, is given below.

- Job management
  - Job scheduling: read and interpret the control cards, allocate computer time, form job queues, handle priorities, load programs, and respond to traps and interrupts.
  - I/O allocation and control: dynamically match and assign I/O channels and devices with job requirements, monitor their status, and control their operation.
  - Operator communication: handle all communications to and from the operator.
  - Error, diagnostic, and recovery processes: discover errors, issue diagnostic messages, and handle system recovery procedures.
  - Utility and miscellaneous services: handle special I/O considerations, intercommunication between terminals, security, sharing of data base considerations, and device-to-device transfers.
  - Audit log: log all system activities for audit and correction and recovery purposes.
- Data management
  - File control: describe a file, input data to a file, maintain the file.
  - Open/close files: open (make available for use) and close files as required by a specific task and limit access and type of access for security reasons.
  - I/O supervision: control the movement of data between elements of storage.
- Task management
  - Task supervision: load the task (a unit part of a program) into main memory for execution, and control the movement of tasks between primary and secondary storage.
  - Interrupt handling: handle all interrupts to the execution stream.
  - Facility and user time accounting: handle accounting of user and system program execution time and of system component use time.
  - Language translation: provide capabilities to assemble or compile source language programs.

The computer operator and user communicate with the computer through the operating system. They use a special language, often called the "job control language" (JCL). Each operating system has its own control language designed to allow the operator or user to direct the operation of the computer. These JCL statements are entered into the computer along with the programs to be executed. The operating system usually loads these JCL records into a storage unit where they wait their turn for processing in what is called a job queue.

Often the JCL statements are loaded onto a disk file when the job is originally created. This file of job control statements is known as a procedure library. Each set of job control statements in the procedure library is given a unique name or number identifier. The user then need only enter a single statement or instruction containing the identifier to cause the operating system to retrieve and execute an entire set of job control statements from the procedure library.

The great majority of computer installations use operating systems supplied by the computer manufacturer, often with operating system options purchased from other vendors. Although the basic operating system must be used to run the computer, the owner decides what options to use. Larger computer installations employ specialists known as systems programmers who maintain and enhance the operating system. They analyze the options and recommend operating system options as needed, maintain the operating system, apply changes received from the operating system vendor, and evaluate and monitor the operating system performance.

The operating system for a mainframe computer usually consists of millions of machine instructions, typically requiring hundreds of person-years to develop and test. Computer operating systems are among the most complex mechanisms ever created by humans and are therefore unpredictable in all circumstances.

Operating systems support several different modes of operation depending on the hardware configuration and the types of work that the computer owner wants to accomplish on the system. These are described in the following sections.

b. Multiprogramming and Multiprocessing

Multiprogramming—Computer processors are much faster than the I/O devices connected to them. In a typical system the speed difference might be:

Device	Data Handling Capacity (characters/second)
Processor	3,000,000 - 10,000,000
Disk drive	600,000 - 3,000,000
Tape drive	100,000 - 2,000,000
Printer	500 - 1,500
Card reader	300 - 1,300
Terminal	30 - 10,000
Person	10 - 50

Early computer processors were usually idle most of the time; they had to wait until one of the input devices passed the next piece of necessary information to it or an output device received the finished information output. Multiprogramming systems were developed to make fuller use of the computer processors by performing other operations asynchronously during the input/output wait times.

Multiprogramming systems permit more than one program or job to be executed simultaneously in the computer. When the program being processed is forced to pause to exchange data with an I/O device, the operating system switches the processor to execute another program until that program also is forced to pause, and so on.

Multiprogramming systems operate under the control of the computer operating systems that perform many functions, including determining which of the several programs will be processed next. In some schemes, the programs are executed in rotation; in others they are executed in order of priority. In the latter scheme, the jobs are ranked when they are entered, and the operating system always attempts to do the highest priority job next. If several programs of the same priority are waiting, the operating system will choose the one that has been waiting the longest time and that will fit in available storage.

When a program has completed its tasks in a multiprogramming system, the operating system releases the space that program has been occupying and begins the task of reading in the next program. This program input task then becomes one of the processor's tasks. To ensure an uninterrupted flow of work to the processor, programs are loaded into the computer as soon as possible. The operating system stores these programs in a reserve area, usually a disk drive, until the necessary processor space and I/O devices are available. Other programs must wait until other requirements are met. Often a single computer job will contain several programs that must be run in a prescribed order. The operating system can initiate the first program in the job, but it must hold the second and subsequent programs in reserve until the first is complete, and so on.

Multiprocessing—Multiprocessing consists of two or more connected processors under the control of a single operating system. This approach provides large computing capabilities. Multiprocessing advantages include the following:

- The interconnected processors can communicate directly with each other.
- Main storage and I/O devices can be shared by the processors and used more fully than if one set is dedicated to one processor and another set to another.
- Only one processor is required to run the operating system.
- Some degree of backup is available for processor failure.

3. Batch Data Processing

Many business applications performed by computer systems occur periodically rather than constantly. For example, hourly workers are paid weekly, or semimonthly, or on some other pay-period basis. The time records that workers submit during the pay period are gathered into a batch. This batch of time records is then processed, payments are made, and year-to-date records are brought up to date in a single job and on a scheduled date.

Most computer systems are used in batch mode. Banks use batch mode to process checks, credit or debit the proper accounts, and produce insufficient funds warnings and monthly statements. Retailers use batch mode to record purchases and on a scheduled date to calculate finance charges and produce monthly statements for mailing. Batch is usually the most economical way to provide periodic processing and to maintain system records that need not contain or reflect up-to-the-minute information.

a. Input Handling

Input for a batch mode is collected during the period between processing runs. For example, weekly time cards for hourly employees are usually gathered from the time card racks once a week and submitted to the computer in a batch. If the worker is paid every two weeks, the payroll is processed with two weekly batches of time cards. In another

case, employees may record their attendance using a clock that automatically records the time, date, and employee number onto a data processing recording device. Again these data are submitted to the computer in a batch, perhaps at the end of each day.

These batches of employee time clock records are called transactions. The first step in handling transactions is to convert them to a computer-processable form. Time cards go through a data entry process that records the information onto a computer input medium, such as punched card, magnetic tape, or magnetic disk. The converted time card records then become the payroll transaction file.

Typically, the payroll transaction file is sent first to a batch computer system that edits or checks for errors. The editing may, for instance, determine that each employee number in the transaction file is for a currently active employee, that no employee overtime is reported without proper authorization, and that one and only one time card exists for each current employee. The edit system produces a new payroll transaction file containing only the correct records and a list of time records rejected for real or possible error. The rejected records are then corrected and entered again through the edit system. This process is continued until the person responsible for payroll decides the computer input transactions are free of error.

b. Processing and File Handling

When the time record input transaction file has been edited, corrected, and cleared for use, the payroll process itself occurs. The time record for each employee is placed in the current hours space in the employee record, the gross and net pay is calculated, and the various outputs including paychecks are prepared. Processing occurs at computer speed; several thousand payroll calculations can be done each minute. Table 22 illustrates the files that might be used in and produced by our simplified payroll example.

The previous payroll master file was produced as output from the last weekly payroll process. The payroll master file output from this week's process will in turn become the input to next week's payroll. In this way, the constantly changing year-to-date records are kept current.

The payroll master file also contains less variable and static information such as social security number and hourly pay rate. To change static information such as the pay rate, a member of the payroll department enters a transaction into a separate process—usually called the master update. New employees are added, names are revised, and other changes are made to the payroll master as in the update process. Typically, every computer file passes through one or more update systems during each processing cycle.

Table 22

EXAMPLE OF SIMPLIFIED PAYROLL FILES

Field Description	Time Record	Old Payroll Master File	New Payroll Master File	Check File
Name	Joe Smith	Joe Smith	Joe Smith	Joe Smith
ID Number	101142	101142	101142	
Hours worked	41	38	41	
S. S. number		363-99-9999	363-99-9999	363-99-9999
Pay rate ($)		5.50	5.50	
Weekly:				
Gross earnings		209.00	225.50	
Taxes		36.11	38.96	
Net earnings		172.89	186.54	186.54
Year to date:				
Gross earnings		2113.55	2339.05	
Taxes		304.04	343.00	
Net earnings		1809.51	1996.05	

Other than transaction files, input master files, and output master files, batch processes also produce other output files such as the check file in the example. The check file can be used for other purposes in addition to printing the paychecks. It may, for example, be used to produce a check register in social security number sequence by sorting the file in the computer to the desired sequence and then printing the required report.

Typically, payroll processes are done in sequence, one employee at a time. This approach is used because all or most of the employees have time record transactions each pay period. In the previous example, the two input files would be arranged in the same sequence, probably employee number, and processed together. These kinds of sequential files are usually kept on magnetic tapes.

Direct-access techniques that store and retrieve information at random can also be used. Computer disk drives are devices that allow direct access to any individual record as the program directs. Files on disk drives can also be read and processed sequentially. In our example, the payroll master might be kept on a disk and updated directly when a few rate changes are made, but it can be retrieved and processed sequentially when the entire file is used to process the payroll.

The discussion thus far has centered on a process that updates one master file at a time. Many systems are designed to update several files at one time with the transactions.

For example, the time-record transaction file can also be used to update a separate file that is keeping track of total hours worked and is not concerned with dollars. This hours file also may be either a sequential or direct-access file.

c. Output Handling

The payroll example given earlier in this section will produce several outputs, including files (e.g., new payroll master file, check file) and reports (e.g., pay checks, check registers, tax reports). Each output must be distributed in a prescribed fashion. The output files are given to the person responsible for the computer center data files. This person, usually called the librarian, records the data, volume number, name and number, and other vital information and stores the file so it can be retrieved when needed next.

The reports are then printed, burst apart, and sent via courier or mail to the proper recipients. Other reports such as the check register might be microfilmed and the film sent to the recipients by the same route.

d. Local and Remote Processing

The three main groups generally involved with payroll—the employees, the payroll department, and computer operations—may be physically near to or far removed from each other. When they are physically adjacent, the data processing is called local or centralized processing; when the groups are physically distant, it is known as remote or distributed processing.

Although local processes usually rely on couriers and mail deliveries to move information, remote processes often must rely on data communications circuits to transmit the data. Remote processing systems typically differ from local processing groups in these ways:

- Input preparation is near the employees and may be separated from the computer processing center.
- Output preparation, printing, and bursting are near the payroll department and may be separated from the computer processing center.
- The systems contain additional checks and edits to make certain the I/O data are correctly transmitted.

Facilities that depend on a distant computer linked by communication circuits perform at least part of their own data processing work. Typically, they have data entry equipment that allows them, for example, to convert time records into computer-readable input transactions as well as printing equipment that can produce output such as checks and check registers. The I/O equipment connects to a data communication circuit in a direct mode or through specialized communications equipment.

In other cases, the I/O equipment includes a computer, which allows the remote facility to do at least part of the processing. Transaction input is partially edited and corrected at the point of entry before it is communicated to the computer center for processing. However, the time card transactions cannot be completely edited unless the payroll master is also available, which usually means the final edits occur during the payroll process in the computer center.

4. On-line Data Processing

On-line data processing systems are designed to perform their processes at or close to the time at which events occur. (The term "real time" is sometimes used in a general sense when referring to on-line systems, but such usage is incorrect; real-time systems are a special class of on-line systems, an example being the process control system described later in this section.) Data processing systems can achieve such timely performance if users have video display terminals (VDTs) or other terminals that are directly connected to the computer system via cables or data communication circuits.

A good example of an on-line system is an airline reservation system. Airline reservation data must be changed very soon after the reservation agent enters the necessary passenger information to prevent another agent from reserving the same seat (perhaps the last available on the flight); the second agent must be advised it is not available. The agents must be able to send information to the computer as sales, cancellations, or changes occur and to determine the status of the reservation data at any time. A design characteristic of such on-line transactions is that the amount of computer processing performed for each transaction instance is usually trivial. Because only a few data accesses are required, the system can respond quickly, typically within a few seconds or less, to all transactions.

Although all transactions occur on line and most data updates occur when received, not all on-line systems are designed to update the information files as transaction information is received. An airline, for example, may enter its employee time records using the reservation agent's terminal. The on-line system receiving the payroll transactions would store them on a payroll transaction file in the computer. This transaction file would then become the input to the batch payroll system at the end of the pay period. The airline might decide to design its payroll information collection system in this way to avoid buying special equipment or to provide daily reports of hours worked by location.

On-line system data files are up to date and accessible to the system at all times. Direct access devices, such as disks, are used in on-line systems to allow the system to access the files in the random order in which access requests are received from the users. Therefore, on-line system master

files are found on disk drives connected to the system when the system is in operation. Because some on-line transactions do not require immediate update of the files, the data on the disks may not reflect the most recent changes.

Time-sharing is an on-line technique that permits more than one system user to share the same computer simultaneously. The number of simultaneous users is limited only by the size of the computer. The computer serves time-sharing users one by one, but allows each one only a brief processing time. In a time-sharing system designed for a limit of 50 users, for example, each might be limited to 1/20th of a second; no one user would have to wait more that 2.5 seconds for service. Because humans take several seconds to act or react, most users would receive a fast response and have the impression they were the only users.

As mentioned in Section IV, scientists and engineers use time-sharing extensively for research and development problem solving. Unlike the on-line transactions described above, however, these types of time-sharing interactions may require significant processing time and many data accesses. Although time-sharing systems can efficiently serve this type of users, response time is of less consequence because of the nature of the interactions. Examples of use of three commercial time-sharing services are presented in Appendix H.

a. Input Handling

Most input is submitted directly to on-line data processing systems. The batching of input documents and the data conversion steps found in batch systems are both avoided. Instead, the person enters each transaction directly into the system with a terminal device, such as a VDT. On-line systems are designed to cause the computer to periodically interrogate each connected terminal device to determine whether it has information ready to be input. This interrogation process is called "polling."

When an affirmative response is received, indicating a terminal is ready to send data, the system initiates actual transmission of the information from the terminal device to the computer. At the end of data transmission, the system may be, and usually is, designed to send an acknowledgment back to the sending device. This message assures the person sending the information that the computer correctly received it.

Immediately following receipt of the information at the computer, the system usually performs the following tasks:

- The information is recorded onto a transaction file called a log. The date, time, and source device are also usually recorded on the transaction log.
- The transaction is edited to make certain the data are acceptable; for example, dates and times must be numeric and names alphabetic. Everything in the transaction must be in a specified sequence.
- Unintelligible transactions are rejected with an error message indicating the reason for rejection, such as "NAME MISSING" or "ACCOUNT NUMBER INCORRECT."

Subsequently, the system performs the required operations on the transaction. There may be one or many types of transactions, each requiring unique handling. The transaction type is often defined by an identifying code in the transaction. In other instances, the terminal devices are designated to send only one type of transaction, and the system determines the type of transaction by identifying the device.

The airline reservation system, for example, must be able to handle many types of transactions. A partial and simplified sample of the possible types of transactions might include:

Transaction Code	Possible Handling
INQ XX	Find the flight record referred to in XX and transmit the information on file regarding that flight to the inquiring device for printing or display. (This is an inquiry.)
RES XX YY-YY	Reserve a seat for the person named YY-YY on flight number XX.
CAN XX YY-YY	Cancel the reservation on flight number XX for the person named YY-YY and make it available for use.
ADD XX ZZ-ZZ	Add flight number XX according to the information in ZZ-ZZ.
DEL XX ZZ-ZZ	Delete the leg or legs of flight XX specified in ZZ-ZZ and list the customers holding reservations who need to be notified.

Note that the functions performed by the INQ, RES, and CAN transactions are the routine business of the reservation agent. However, reservation personnel do not add or delete flights and therefore do not need to be authorized to use the ADD and DEL transactions. The use of the ADD and DEL transactions would be limited to designated authorized parties, such as flight operations personnel. To prevent any party from entering unauthorized transactions, several techniques are available, including limiting the entry of these transactions to certain physical devices or requiring users to enter a secret password to authenticate their identity.

On-line systems also receive a part of their data from batch processes. Often, 24-hour-a-day systems, such as airline

reservation systems, are fully stopped once each day. The following batch functions may be performed during this period:

- The file of connected terminal devices and flight schedules is changed by loading in a new batch of data identifying the terminals and flights that will be available during the next 24 hours.
- The transaction log is terminated, removed from the computer, and processed to create operating reports.
- The application and system files are copied, and the copy is removed from the computer and stored in a safe place.

b. File Handling

On-line systems contain several types of files, including:

- Reference files containing basic information the system needs to operate, including the identification of system users and devices accessing the systems. These files are used frequently and are usually stored in computer memory for fast access.
- A log file recording all transaction inputs sequentially as they occur.
- Master data files, usually on a direct-access disk drive, that contain the data being used and updated by the system users.

These files constitute the on-line system data base. On-line data processing systems often use a DBMS to access the system data base.

As noted earlier, the reference files are periodically loaded into the system, often when the system is started up at the beginning of a processing period, such as a day. Certain changes may occur during the period that affect the reference files. A terminal device may fail, for example, and the system will be unable to send or receive information to that device. On-line systems are usually designed to shut down the failing device and notify computer operations personnel. The reference file of terminal devices is annotated to indicate one is inoperable. The system will then no longer poll the inoperable device to determine whether it is ready to send or receive information. When the problem has been corrected, computer operations personnel enter a special transaction that restores the device to the polling sequence by removing the inoperable annotation from the reference file.

Recovery and Restarts—The transaction log file produced by the system records all transaction information entered as well as other identifying information, including time and place of origin. The log file is a valuable source for volume statistics, but its primary purpose is to permit the system to recover after a failure that destroys the data base or makes it inaccessible to the system. When that situation develops, the system's users are not allowed to access and use the system until the data base has been restored to its correct status just prior to the failure.

The computer operations staff restores service by executing a computer program that recovers all the necessary information. The copy of the data base as of the beginning of the processing period and the transaction log for the period are inputs to a recovery program that repeats all the transaction processing up to the point of failure without, however, sending output information to the terminal devices again.

These recovery processes are time-consuming; in many situations, however, keeping the system operational all or nearly all of the time is essential. Airline reservation agents are nearly helpless when their reservation system is inoperable, and customers may go to another airline that can immediately reserve a seat on a competitive flight. Various techniques are used to reduce recovery times to the shortest feasible interval, including frequently saving transaction log and data base copies to reduce the amount of processing necessary to restore the data base. When it is economically feasible, the entire system is duplicated on a standby computer that is ready, complete with separate copies of the data base, to take over system processing if anything goes wrong on the primary computer.

Design Alternatives—The data base is the focus of on-line systems. The systems are designed to keep the data up to date and to extract the information from the data base as required to support the system users' needs. The airline reservation system keeps the reservation file up to date to the last transaction.

Credit card companies may be less precise in updating transactions. Instead, they normally update their customer files at night in relatively inexpensive batch mode. These companies mail customer charge slips and payments to the computer center; therefore, the most recent several days' transactions may not be reflected on their files. Nonetheless, they maintain on-line systems that allow users to access the credit card customer files to determine that the account is valid and that a customer's new purchase will not exceed the credit limit.

The credit card companies would undoubtedly prefer to charge the customer's account immediately after each purchase. This capability would allow them to guard against shopping sprees by a criminal who has just gotten possession of the card. However, immediate updating would require each sales station to be connected to the computer by a communication circuit. Although credit card authorization is performed on line, on-line capture and updating for individual purchase are limited.

Updating Techniques—Two approaches are used to keep files up to date at all times in on-line systems—memo-posting and update-in-place. Memo-posting systems do not actually change the information on the system data base. Instead, the transaction information is stored in a separate memo file when it is received at the computer, and the data base is annotated to indicate that a change has occurred and often where the change can be found in computer storage. If a second transaction is received, another annotation is made—usually in the first transaction record in storage. This structure allows the system to determine at any time the total amount a customer owes and his remaining credit.

Memo-posting systems require batch programs that periodically create a new, up-to-date data base and to eliminate the annotations. In credit card applications, the batch programs are run at night when the on-line system is idle. Credit card batch systems also record the transactions onto a log file and save them for inclusion in the next monthly customer statement.

Update-in-place systems perform the same functions and provide the same capabilities as memo posting; however, the design approach is different. The data base is updated each time a transaction is received and no annotation is necessary. However, a record of the transactions must still be kept, not only for the eventual production of the customer's statement, but also for the restoration of the master file if it should be destroyed during the day's operation through computer operator error, equipment malfunction, or other failure. The update-in-place and memo-update approaches are sometimes used together in a system, with some files handled one way and other files handled the other way.

c. Output Handling

Batch systems often produce large printed or microfilmed reports, which the user can store and retrieve for reference purposes when necessary. The search time, especially on printed reports, can be substantial. On-line systems are designed so that the computer searches its storage and provides the user with the information needed and no more. Airline customers are interested only in their own travel routing, and the reservations agent serving them usually need look no further to accommodate their needs. Thus, the reservation agent requests and gets information on the 130 seats on one flight, not the many thousands of additional seats that may also be available in the airline system.

On-line output is usually produced in the form of displays on a terminal screen. This display might contain, for example, the number of available seats on Flight 83 bound for Duluth, or Sally Smith's credit limit and unused credit amount. The display content is designed to meet the specific need of the requester, and the requester defines this need to the system by entering a transaction code and data that will provide the information required to uniquely identify the request.

If a printer is available, display information can also be printed. Printers are electro-mechanical and often much slower than display units of the same cost. Although they are used sparingly, if at all in most on-line systems, some on-line systems are specifically designed to provide printed reports. The most common are message systems that move or switch typewritten information entered at one location to one or more other locations at electronic speeds. Most message-switching systems now use a computer to receive, validate, and dispatch the messages.

Documents may be optically scanned and input, stored, and printed or displayed in graphical form such as for facsimile (FAX) transmission or for on-line processing of image data such as pictures. Conversion of graphical text and voice into their logical text content is also increasing.

Confidential or sensitive information that a computer batch system prints is safeguarded by limiting access to the printed report, often by locking it up when it is unattended. Because many on-line systems can also display confidential information in many locations at once, each user with access to the on-line system becomes a guardian of the information received. Therefore, confidential and sensitive information is usually made available to only a few authorized individuals who are issued a special password known only to them and the computer; the terminal they use may also be located in a secure area. The on-line security problem has never been completely solved.

5. Process Control Systems

Process control and process monitoring systems are true real-time computer systems used to measure and control external processes and operations. In many cases, the systems measure one or more current conditions with respect to limits programmed into the system, and they feed back signals that adjust the operation of the system to keep those conditions within limits. These feedback or "closed loop" systems are called process control systems. In other cases, there is no feedback; instead, the system only reports and records out-of-limit situations. These are process monitoring systems. For convenience, both control and monitoring systems are called process control systems.

a. Input and Output

Process control systems are designed to control and monitor processes such as physical, nuclear, electrical, or chemical plants through electronic devices connected to a computer. Examples of these devices include limit switches, photocells, scales, and thermometers. These input devices constantly measure the variables over a range of

values. These are called analog measurements. An "analog to digital converter" placed between the sensing device and the computer converts analog input signals to digital values. The computer periodically records the digital measurements as specified by the computer program. A thermometer reading may be recorded 100 times per second while a movement-sensing photocell connected to the same process might be checked and recorded 500 times per second.

Process control system output goes to devices such as solenoids and motor starters connected to the computer through a converter—in this case digital to analog. Basically, the converter changes a digital signal from the computer into an electric current that activates a physical device.

Process control systems can also receive and send digital information. Typically, such systems include output display units that constantly show the state of the connected process or operation, and often include logging devices that print the information for later analysis or reference.

b. Processing

A program that controls and/or monitors a process is typically interrupt or signal driven; that is, it basically sits in an idle state until it is required to perform some function. The interrupts or signals may come from internal or external sources. An example of an internal interrupt is the interval timer that periodically wakes up the idle processor and indicates that a sensing device should be read. An external interrupt example would be an alarm signal generated by a sensing device indicating an out-of-limit condition. Because this condition is not predictable and can occur asynchronous with other events, it must be handled immediately. Clearly, the interrupts or signals must each have an assigned priority and the computer program must handle them in priority sequence.

Process control computers are also designed to provide clear warnings and calls for assistance when they fail. Warning devices such as horns, bells, or warning lights are automatically activated if the computer shuts down. These computers may also be programmed to automatically shut down the processes or operations they control to prevent equipment or product damage or human injury.

c. Applications

Process control systems have an almost endless variety of uses. Such systems might be found at work in a modern industrial plant performing such tasks as:

- Access control—controlling access to the premises through badge-reading devices and gate activators.
- Environment control—turning space heaters on or off as required and controlling the heat circulation system.
- Material handling—operating high-rise stacker cranes in warehouses to store and retrieve containers of materials.
- Machine tending—running machines through their cycles and activating the devices that feed raw material into and extract finished goods from them.
- Quality control—constantly measuring the quality of goods being produced, rejecting the bad items, and shutting down malfunctioning processes.

In these industrial plant examples, several computers of the same or different design or make might be used. Each use requires a different set of I/O devices, a different computer program, and all or part of the capacity of a computer.

Increasingly small and more powerful microprocessors are being used in the office and home in a manner similar to process control systems. Telephone switchboards and automatic typewriters are two common office uses of microprocessors. They are also found in electric appliances, washing machines, television sets, and automobiles. The computer program contained in the microprocessor is designed and programmed at the same time as the product in which it will be used. Programs are loaded into these computers during their manufacture and cannot be changed thereafter except by substituting a component of the processor.

C. Data Communications and Teleprocessing

1. Communications Concepts

Data communications is defined as the transmission of digitized and computer processable information via communications circuits from one location to another. Teleprocessing is a form of data processing that uses data communications.

Data communications and teleprocessing are used when the processing computer needs to be physically separate from the source of the input data, the site of the output usage, or the computer user. An airline reservation system is a common example. Reservation systems use data communications equipment and techniques to connect travel agents and airline personnel to a single computer or set of computers that is continually recording reservations, answering space availability inquiries, and performing necessary control tasks.

High-capacity cables, capable of carrying hundreds of thousands of characters of information a second, connect computers to high-speed machines such as other computers, disk drives, and tape drives. However, many machines connected to computers operate at much slower

speeds. These slower machines are connected to the computer by lower capacity, less expensive cables similar to telephone lines. Direct cable connection becomes impossible at distances of more than 1 mile and usually becomes inefficient after 2,000 feet. When users miles away are communicating directly with a computer, they are said to be connected via a data communication circuit.

There are two types of data communications circuits—analog and digital. The voice telephone network typically uses analog circuits capable of transmitting the full range of sounds that the human voice is capable of making. Similarly, the hands on a clock face can portray the full range of minutes in a 12-hour period. Analog communication is constantly variable within a predetermined range of frequencies.

Digital communication circuits use the binary on-off principle to communicate information in digital form. A computer can convert sound into a series of digits that portray the volume, pitch, and other distinguishing characteristics. These digits can then be reconverted into sound by another computer at the receiving end. Digital circuits can move more information over a given distance in a given time than analog circuits and eliminate the noise distortion problems common to sound-carrying circuits. In many areas, digital circuits are replacing analog circuits in the telephone system.

Data are transmitted at the speed of electricity, but one bit at a time. Typically eight bits are required to transmit each character. A normally functioning voice circuit is theoretically able to transmit 9600 bits per second, or 1200 characters per second, but the effective transmission rate is about 1000 characters per second. For comparison, people read at 50 bits or 6 characters per second and type at 15 bits or 2 characters per second. Slower transmission speeds are often used so that slower and less expensive equipment can be used at each end of the circuit. Transmission rates much higher than 9600 bits per second, up to several million bits per second, are also possible on special circuits available from communication carriers.

Transmission errors occur frequently, usually when the communication circuit is momentarily disrupted. These disruptions often destroy some of the bits being transmitted thereby causing a condition known as a parity error (counts of the number zeros and ones are not correct). The receiving equipment detects these parity errors and then notifies the communications control program in the central computer that an error has occurred. This program takes the necessary corrective action, usually retrying the transmission until error-free data have been achieved.

Digital information to be transmitted on analog circuits is first converted to analog signals by a special device known as a modem (MOdulator-DEModulator), then reconverted to digital information by another modem at the receiving end. The analog circuits are obtained from a common carrier, usually the local telephone company. Data communications circuits may be regular dialed telephone lines or dedicated lines leased from a communications carrier. Leased lines cannot access or be accessed by the dial-up network. Modems are required at each end of both types of lines to perform the necessary digital-analog-digital conversion.

When all digital circuits are used for data transmission, a different device is required at each end of the circuit similar to modems on analog circuits. This device is called a CODEC (COder, DECoder) and basically codes or decodes the information being transmitted.

The two basic methods for transmitting information are known as asynchronous and synchronous. Asynchronous uses a starting bit for information, followed at regular timed intervals by the bits representing a character, followed by another start bit and so on. This is the least expensive and most widely used transmission method for low-speed systems.

The synchronous method uses a process called "handshaking" during which the sending and receiving device establishes a common clocking rate and transmits thereafter at the intervals specified by the clocking rate and without the need for the starting bits. The sending and receiving ends are said to be synchronized. Synchronous equipment requires internal clocking and is more expensive, but synchronous transmission does not need the starting bits to separate characters and it is faster.

A number of communications protocols have been designed for use in the synchronous environment. A communciations protocol defines the format and characteristics of the data that are transmitted. For example, raw data received for transmission are divided into segments or packages, typically of fixed length. Each package of data is enclosed in an "envelope" with a header containing information about the package, such as data length, address of destination, and error detection information, and possibly a trailer specifiying other information. The communications protocol rigorously and formally defines the format and content of this packaging and also specifies error handling and other characteristics.

An example of a widely used communications protocol is SDLC (Synchronous Data Link Communications). IBM developed SDLC as part of its Systems Network Architecture (SNA), which establishes the ground rules and defines the common interfaces for data communication between all IBM-developed computer systems. Because of its wide use, SNA/SDLC is a de facto standard within the data processing industry and has been adopted by other computer and communications equipment vendors as well.

The International Standards Organization (ISO) has also developed and published an internationally accepted set of standards known as the Open Systems Interconnect (OSI), a seven-layer communications architecture that is functionally similar to SNA. OSI consists of a suite of protocols that define, or will eventually define, the several layers. Standards have been published defining the first three layers of the architecture; discussions are ongoing concerning the remaining layers. The second layer, link control, is defined by HDLC (Higher-Level Data Link Control), a synchronous protocol very similar to SDLC.

Perhaps the best known of the ISO/OSI protocols is the X.25 standard, which defines Layer 3, Network Control. X.25 defines networks that are known as packet-switched networks. In these networks, messages are divided into packets at the sending site and transmitted one packet at a time. The route from the message's origin to its destination may be a simple, point-to-point routing, or it may be complex, going from node to node (a node is a location on the network that may send or receive messages) before reaching its final destination. As each packet reaches, for example, node A, the packet is switched to the next node along a path to its destination. Depending on the network configuration and availability of links, there may be several paths to the destination and each of the individual packets could take a different path to reach the same final node. For example, a message sent from New York to San Francisco may go through Chicago, Denver, St. Louis, or Dallas. A four-packet message might have one packet routed through each of these locations. In this type of network, packets may arrive out of order in an asynchronous fashion, and must be properly reassembled to complete the message. All the details necessary to handle these and other complex situations are rigorously defined in the protocol.

Other computer vendors have developed similar communications architectures—Digital's DECNET is a good example. In general, however, most businesses accept and are implementing either IBM's SNA or the OSI model. Developments over the last few years indicate that these two communications architectures will slowly but surely converge to a common point.

As with data base technology, a detailed coverage of communications is beyond the scope of this manual. Many good reference works dealing with this subject are available [39].

2. Communications Carriers

Communications carriers are the companies that supply facilities for transmitting analog and digital information. Several federally regulated companies provide most data communications services in the United States, using the existing voice facilities. The best known are the former telephone operating companies of the AT&T system, the RBOCs (Regional Bell Operating Companies), as they are known.

Other communications carriers often specialize in data communications and compete with or supplement the telephone company networks. Western Union, GTE, and MCI are among the better known competitors licensed to operate as communications carriers within the United States. These and other firms also supply international data communications services.

Carriers use a variety of technologies including high-data rate microwave facilities, satellites, fibre optics, and radio systems. Most carriers use several or all of these technologies, and a single signal may travel over land line, microwave, radio, and land line again before it completes its journey.

Another class of common carriers offers what are known as "value-added networks." The value-added carriers such as Tymnet or GTE Telenet provide packet-switched network services using common carrier facilities and specialized data communications equipment. In addition to data communication, these carriers provide other services that add value to simple communications capabilities. Examples include conventional data processing services as well as specialities such as credit card authorization.

3. Teleprocessing

As noted earlier, data communications systems are used to connect computer users to a physically distant computer center. Those users type at 15 bits per second and read at 50 bits per second. They are connected to the computer via a data communications circuit that typically operates at speeds of 2400 to 9600 bits per second. The computer itself operates at speeds of hundreds of millions of bits per second. Obviously, one user can use only a small portion of the communications circuit capacity and only a tiny fraction of the computer's capacity. Data communications systems are designed to use the excess computer and circuit capacity in several ways to reduce the overall cost.

Communication link costs are minimized by a design known as "multidropping." Many users at one place or in a geographic region are connected to a single communication line. As in a party line phone system, each user's machine has a unique name or address. The computer calls each in turn to see if it is ready to receive or transmit data. This technique is known as "polling" and data communications lines designed in this manner are known as multidrop.

Computer costs are minimized by allowing many users to share the same computer. A typical small computer can

simultaneously operate several data communications lines at one time and larger computers can simultaneously work with hundreds. The amount of work the computer must do to satisfy its users and the computer's processing speed determine the capacity limit of these types of systems.

On-line data processing systems operate under the control of a special operating system program known as a "teleprocessing monitor." This program controls the transfer of information between the communication lines and the computer's storage and often does the user polling as well. In other cases, specialized computers known as "front-end processors" are used to control the data communications, especially polling, and to notify the main computer when and if information exchange is needed. Front-end processors are used to reduce the work load on the main computer, thereby enabling it to serve more lines and users.

Users may also be connected indirectly to a central computer, either through another computer located miles away or through other higher speed machines such as computer tape drives or high-speed printers and card readers. These computer-to-computer and computer-to-higher speed machines are not bound by the speed of users at their individual slower speed machines. Instead, whole processing jobs are performed without user intervention or interaction. These types of systems are known as remote job entry (RJE). Typically these systems operate at much higher speeds and consume an entire communication line when operating. Therefore, lines are leased and dedicated for each RJE site.

The central computer also plays a key role in communications with the users who are indirectly connected. The communication occurs under the control of a special program in the central computer known as a "spooler." The records received from the user's machine must be immediately stored within the central computer in an input queue. Similarly, output from the central computer to the user's machine must be put in another storage area called the output queue. This system allows the user's machine to be a relatively simple and inexpensive device capable of performing only one function at a time. The user can schedule the work to and from the queues when ready and need not wait for the central computer.

a. Terminals

Terminals are machines that can send and/or receive digital information over a communication circuit. They may be attached by a long-distance circuit many miles long. Terminals are the users' means to send information to and receive information from a computer or another terminal, whether nearby or far away. Terminals may or may not have the ability to store information; some may include a small computer for handling a few functions independent of the central computer.

The five major kinds of terminals have the following capabilities:

- Typewriter-like terminals much like teletypes. These include a keyboard for entry of information and a printing device. These terminals supply a printed copy of what the computer sends back and usually of what the terminal operator has entered as well, but are slower and slightly more expensive than display terminals.
- Display terminals, also known as VDTs. These include a keyboard for entry of information and a screen resembling a television set for displaying information. These terminals are fast and easy to use, but cannot supply a printed record of the information. If a printed record is necessary, a printing terminal must be added to the system. Display terminals are inexpensive and widely used.
- Intelligent terminals using a small computer. These terminals may have a wide variety of means for entering and receiving information; they can do local processing as well as store and retrieve information. These are the most versatile terminals but are also more expensive.
- RJE terminals, usually a card reader and a high-speed line printer. These are used when high volumes of I/O must be handled (e.g., nearly always in a batch operation, such as a weekly payroll).
- Specialized terminals, including a wide variety of specially designed devices for entering and receiving information. Examples are cash-dispensing machines, timekeeping terminals that can read and verify an employee's identification badge, special printers that prepare airline ticket stubs, and graphics terminals for scientific and engineering users. Specialized terminals are more expensive to engineer than standard terminals and are usually found in large organizations with an unusual combination of terminal requirements and a need for many such terminals that can absorb the engineering costs. Examples are airlines, major banks, and large facilities with stringent security requirements.

b. Computer Networks

The preceding discussion of data communications assumed the existence of only one computer installation connected to local and remote users. However, some organizations need to interchange information among physically separated computers. The resulting complex of multiple computers equipped to move information from place to place using communication lines is known as a "computer network."

Computer networks are rapidly gaining acceptance as a faster, more economical method for moving information

from one organization to another. A prominent example is the banking industry, which routinely transfers trillions of dollars by means of computer-to-computer transactions via a network known as the electronic funds transfer system (EFTS). EFTS is performed internationally through SWIFT, a system that is cooperatively funded and operated by financial institutions in many nations.

Many large businesses and other organizations are establishing large, private networks to meet their business requirements. These typically nationwide networks may include several mainframe computer centers as nodes on the network as well as thousands of terminals accessing these computers. By combining the computer networks and terminal networks of the organization, these wide area networks (WANs) are normally accessible only by members of the organization and a limited number of other outside users.

Electronic data interchange (EDI) is an example of outside user access to an otherwise private network. Primarily used in manufacturing and distribution companies, EDI involves the electronic transmission of several types of official documents, such as purchase orders and bills of lading, between participating companies according to established standards. The growing use of EDI and similar communications functions creates interesting and unique security and control problems for data center management.

4. Local Area Networks

The proliferation of personal computers and intelligent workstations in the workplace generated a requirement for linking these devices to each other and to commonly used peripheral devices that was not satisfied by available communications network products. The local area network (LAN) was developed to meet this and other requirements. LANs are marketed by a wide variety of companies for practically every type of personal computer or workstation. The implementations vary considerably from vendor to vendor.

A typical LAN consists of a relatively small number of workstations (usually less than 50) located geographically close to each other in an office or small department. The workstations are connected in a ring by communication links, typically coaxial cable or telephone-type lines. One of the workstations, or a special, dedicated file device, usually serves as a file server or primary storage device for the network. Other server devices, such as printers and gateways to mainframe computer systems, may also be connected to the LAN.

Each workstation uses LAN-specific software to communicate with the other workstations and the servers. Typical functions offered by LAN vendors include electronic mail, file transfer, and backup and recovery facilities. Early LAN implementations paid little attention to security and control, and thus the data stored on them were quite vulnerable to unauthorized access. More recent LAN products have addressed security and control issues. The somewhat informal nature of LAN use, however, still makes them more vulnerable than traditional computer systems.

The Ethernet, developed by Xerox Corporation, is perhaps the most well known example of a LAN. Another popular LAN is the Token Ring Network available from IBM.

D. Computer Security

Unlike today, users of early generations of computers had essentially free rein to use the systems as they wished. Practically anybody with access to a terminal could log on to any early time-sharing system and peruse any of the files on the system. Outside of the defense community and others concerned with national security there was little, if any, concern regarding the computer system's security.

The recognition by businesses and other organizations that the information contained in their computers was an extremely valuable resource and, as such, should be protected like other resources has dramatically changed this situation. Most data processing organizations now have an individual or a group that specializes in the protection and control of computer resources. Corporate auditors and CPA firms have EDP audit specialists on their staffs dedicated to examining computer systems and application software for compliance with prudent security and control practices. Computer vendors and others have developed and successfully marketed security products for practically all computer models.

1. Access Control Software

An access control software package is the most common security product found in commercial data processing organizations, particularly in an IBM mainframe environment where three major packages are widely used. IBM supplies one, the Resource Access Control Facility (RACF); the others, Top Secret and ACF2 (Access Control Facility), were developed independently but are now owned and marketed by Computer Associates, a major software company.

The functions offered by all of these packages are basically the same; the primary differences are in implementation. In general, access control software enables a computer security administrator to restrict access to computer resources to individuals specifically authorized to use them. In addition, they provide audit log accesses, exception or violation reports, and other special security reports. A user is assigned a unique identification (user ID); a valid user

ID, authenticated by a secret password, is required for all access to the system. The password systems provided are generally similar to those described in Section IV. Each user ID has a corresponding profile defined to the access control software that specifically identifies all programs and files (data sets) that the user may access.

When properly installed and administered, an access control package can provide very good control of IBM mainframe computer resources. Similar packages exist for other vendors' mainframe computers and for many minicomputers. Access control software is available for personal computers, but has fewer functions because they are single-user systems.

2. Encryption

Encryption is generally defined as "scrambling" or changing data so that its meaning cannot be determined without the information that was used to change it. Typical uses of encryption are to secure sensitive data stored on disks and other media and being transmitted over communication lines. For example, the PIN (personal identification number) used for ATM transactions is encrypted by the ATM before sending it to the host computer.

In simple terms, encryption is performed by algorithmically transforming the data using a secret parameter called a key. Encryption algorithms can be simple or extremely complex, depending on the security requirements of the data. The U. S. National Bureau of Standards publishes an encrytion algorithm called DES, or Data Encryption Standard. DES is claimed to be unbreakable and is widely used throughout the world.

Until recently, encryption was seldom used outside of the defense and national security community. Outside of the financial industry, it is still not widely used in business. As electronic business transactions (e.g., EDI) expand, however, the routine use of encryption in business is also expected to increase.

REFERENCES

1. Donn B. Parker, Susan H. Nycum, and S. Oura, "Computer Abuse," SRI International, Menlo Park, California, report distributed by National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia (1973).
2. Abraham Ribicoff, "Computer Abuse Control Bill," press release, January 25, 1979.
3. Donn B. Parker, *Fighting Computer Crime* (Charles Scribner's Sons, New York, New York, 1983).
4. Brandt Allen, "Embezzler's Guide to the Computer," *Harvard Business Review*, p. 53 (July 1975).
5. Donn B. Parker, *Managers' Guide to Computer Security* (Reston, Virginia, Prentice-Hall, 1983).
6. Donn B. Parker, *Computer Crime: Computer Security Techniques*, U.S. Department of Justice, Bureau of Justice Statistics, Washington, D.C. (1985).
7. U.S. Senate Committee on Government Operations, "Problems Associated with Computer Technology in Federal Programs and Private Industry," U.S. Government Printing Office, Washington, D.C. (June 1976).
8. U.S. Senate Committee on Government Operations, "Staff Study of Computer Security in Federal Programs," U.S. Government Printing Office, Washington, D.C. (1977).
9. Donn B. Parker, "Prosecutors' Experience with Computer-Related Crime," SRI International, Menlo Park, California (1979).
10. Susan H. Nycum and Donn B. Parker, "Prosecutorial Experience with State Computer Crime Laws," Gaston, Snow, & Ely Bartlett, Palo Alto, California, and SRI International, Menlo Park, California (1985).
11. Albert J. Reiss, Jr. and Albert D. Biderman, *Data Sources on White Collar Lawbreaking*, National Institute of Justice, Washington, D.C. (September 1980).
12. *Tracking Offenders: White Collar Crime*, Bureau of Justice Statistics, Special Report No. NCJ-102867, Washington, D.C. (November 1986).
13. *White Collar Crime: Federal Offenses and Offenders*, Bureau of Justice Statistics, Special Report No. NCJ-106876, Washington, D.C. (September 1987).
14. *Data Report, 1987*, Bureau of Justice Statistics, Report No. NCJ-110643, Washington, D.C. (April 1988).
15. Donn B. Parker, *Crime by Computer* (Charles Scribner's Sons, New York, New York, 1976).
16. Ulrich Sieber, *The International Handbook on Computer Crime*, (John Wiley and Sons, New York, New York, 1986).
17. William D. Young and John McHugh, "Coding for a Believable Specification to Implementation Mapping," *Proceedings of IEEE Symposium on Security and Privacy*, pp. 141-142 (April 1987).
18. B. L. Lampson, "A Note on the Confinement Problem," Xerox Palo Alto Research Center, Palo Alto, California (1977).
19. August Bequai, *Computer Crime: Expert Witness Manual*, U.S. Department of Justice, Bureau of Justice Statistics, Washington, D.C. (1980).
20. Russell E. Brooks, "Expert Witnesses, Used Properly, Can Expedite Fact-Finding Process," *The National Law Journal*, p. 20 (September 5, 1988).
21. James Martin, *Security Accuracy and Privacy in Computer Systems*, (Prentice Hall, New York, New York, 1976).
22. "Common Body of Knowledge for Internal Auditors," Institute of Internal Auditors, Altamonte Springs, Florida.
23. "Standards for the Professional Practice of Internal Auditing," Institute of Internal Auditors, Altamonte Springs, Florida.
24. "Statement of Principle and Standards for Internal Auditing in the Banking Industry," Bank Administration Institute, Park Ridge, Illinois.
25. *Systems Auditability and Control Study*, three volumes, Institute of Internal Auditors, Altamonte Springs, Florida (1978).
26. "Statement on Auditing Standards No. 3: The Effects of EDP on the Auditor's Study and Evaluation of Internal Control," American Society of

Certified Public Accountants, New York, New York (1977).

27. "Codification of Auditing Standards and Procedures," American Society of Certified Public Accountants, New York, New York (1973).

28. Donn B. Parker, "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems," *Proceedings of 1976 National Computer Conference* (AFIPS Press, Arlington, Virginia, 1976).

29. U.S. Senate Subcommittee on Criminal Law and Procedures, "Hearings on the Federal Computer Systems Protection Act (S1766), June 21 and 22, 1978," U.S. Government Printing Office, Washington, D.C. (1979).

30. Donald R. Cressey, *Other People's Money*, p. 147 (Wadsworth Publishing Co. Inc., Belmont, California, 1971).

31. "Annals of the History of Computing," American Federation of Information Processing Societies, Arlington, Virginia (1979).

32. Stanley S. Arkin, editor, *Prevention and Prosecution of Computer and High Technology Crime*, (Mathew Bender, Times Mirror Books, New York, New York, 1988).

33. Leslie F. DeLashmutt, Jr., Captain USAF, "Steps toward a Provably Secure Operating System," U.S. Department of Defense, Washington, D.C. (1979).

34. Richard A. DeMillo, Richard J. Lipton, and Alan J. Perlis, "Social Processes and Proofs of Theorems and Programs," *Communications of the Association for Computing Machinery*, Vol. 22, No. 5, pp. 271-280 (May 1979).

35. Koba Associates, *Computer Crime: Legislative Resource Manual*, U.S. Department of Justice, Bureau of Justice Statistics, Washington, D.C. (1980).

36. Kent W. Coulton, *Computer Crime: Electronic Fund Transfer Systems and Crime*, U.S. Department of Justice, Bureau of Justice Statistics, Washington, D.C. (1982).

37. C. J. Date, *An Introduction to Database Systems*, third edition (Addison-Wesley Publishing Co., Reading, Massachusetts, 1981).

38. James Martin, *Computer Data Base Organization*, second edition (Prentice Hall Inc., Englewood Cliffs, New Jersey, 1977).

39. James Martin, *Design and Strategy for Distributed Data Processing* (Prentice Hall Inc., Englewood Cliffs, New Jersey, 1981).

40. American Bar Association, *Report on Computer Crime*, ABA Task Force on Computer Crime, Section of Criminal Justice (June 1984).

APPENDIX A

Selected State and Federal Computer Crime Statutes

APPENDIX A: Selected State and Federal Computer Crime Statutes

Florida
Chapter 815. Computer-Related Crimes [New]

815.01 Short title

The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

815.02 Legislative intent

The Legislature finds and declares that:

(1) Computer-related crime is a growing problem in government as well as in the private sector.

(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.

(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.

(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

815.03 Definitions

As used in this chapter, unless the context clearly indicates otherwise:

(1) "Intellectual property" means data, including programs.

(2) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

(3) "Computer" means an internally programmed, automatic device that performs data processing.

(4) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(5) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

(6) "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

(7) "Computer system services" means providing a computer system or computer network to perform useful work.

(8) "Property" means anything of value as defined in S.812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

(9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

815.04 Offenses against intellectual property

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in S.812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(4) (a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

815.05 Offenses against computer equipment or supplies

(1) (a) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

2. If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the third degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

(2) (a) Whoever willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

2. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000, then the offender is guilty of a felony of the third degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

3. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, then the offender is guilty of a felony of the second degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

815.06 Offenses against computer users

(1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

(2) (a) Except as provided in this subsection, an offense against computer users is a felony of the third degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

(b) If the offense is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in S.775.082, S.775.083, or S.775.084.

815.07 This chapter not exclusive

The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the

criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

Colorado
Article 5.5 Computer Crime

Sect. 18-5.5-101. Definitions

As used in this article, unless the context otherwise requires:

(1) To "use" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(2) "Computer" means an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

(7) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, or marketable security.

(8) "Property" includes, but is not limited to financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

18-5.5-102. Computer crime

(1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of: devising or executing any scheme or artifice to defraud, obtaining money, property, or services by means false or fraudulent pretenses, representations, or premises, or committing theft, commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than fifty dollars, computer crime is a class 3 misdemeanor; if fifty dollars or more but less than two hundred dollars, computer crime is a class 2 misdemeanor; if two hundred dollars or more but less than ten thousand dollars, computer crime is a class 4 felony; if ten thousand dollars or more, computer crime is a class 3 felony.

Arizona
Criminal Code, Section 13-2316

Definitions

For the purposes of Section 13-2316:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network.

(2) "Computer" means an electronic device which performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such a computer system.

(5) "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected computer equipment, devices and software.

(7) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, marketable security or any other written instrument, as defined by S. 13-2001, paragraph 7, which is transferable for value.

(8) "Property" means financial instruments, information, including electronically produced data, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

(9) "Services" includes computer time, data processing and storage functions.

Section 13-2316. Computer fraud; classification

A. A person commits computer fraud in the first degree by accessing, altering, damaging or destroying without authorization any computer, computer system, computer network, or any part of such computer, system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises.

B. A person commits computer fraud in the second degree by intentionally and without authorization accessing, altering, damaging or destroying any computer, computer system or computer network or any computer software, program or data contained in such computer, computer system or computer network.

C. Computer fraud in the first degree is a class 3 felony. Computer fraud in the second degree is a class 6 felony.

Texas
Chapter 33. Computer Crimes

Sect. 33.01. Definitions

In this chapter:

(1) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(2) "Computer" means an electronic device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device. "Computer" includes a network of two or more computers that are interconnected to function or communicate together.

(3) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(4) "Computer security system" means that the design, procedures, or other measures that the person responsible for the operation and use of a computer employs to restrict the use of the computer to particular persons or uses or that the owner or licensee of data stored or maintained by a computer in which the owner or licensee is entitled to store or maintain the data employs to restrict access to the data.

(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, and punchcards, or may be stored internally in the memory of the computer.

(6) "Electric utility" has the meaning assigned by Subsection (c), Section 3, Public Utility Regulatory Act (Article 1446c, Vernon's Texas Civil Statutes).

Sect. 33.02. Breach of Computer Security

(a) A person commits an offense if the person:

(1) Uses a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer and the actor knows that there exists a computer security system intended to prevent him from making that use of the computer; or

(2) Gains access to data stored or maintained by a computer without the effective consent of the owner or licensee of the data and the actor knows that there exists a computer security system intended to prevent him from gaining access to that data.

(b) A person commits an offense if the person intentionally or knowingly gives a password, identifying code, personal identification number, or other confidential information about a computer security system to another person without the effective consent of the person employing the computer security system to restrict the use of a computer or to restrict access to data stored or maintained by a computer.

(c) An offense under this section is a Class A misdemeanor.

Sect. 33.03. Harmful Access

(a) A person commits an offense if the person intentionally or knowingly:

(1) Causes a computer to malfunction or interrupts the operation of a computer without the effective consent of the owner of the computer or a person authorized to license access to the computer; or

(2) Alters, damages, or destroys data or a computer program stored, maintained, or produced by a computer, without the effective consent of the owner or licensee of the data or computer program.

(b) An offense under this section is:

(1) A Class B misdemeanor if the conduct did not cause any loss or damage or if the value of the loss or damage caused by the conduct is less than $200.

(2) A Class A misdemeanor if the value of the loss or damage caused by the conduct is $200 or more but less than $2,500.

(3) A felony of the third degree if the value of the loss or damage caused by the conduct is $2,500 or more.

Sect. 33.04. Defenses

It is an affirmative defense to prosecution under Sections 33.02 and 33.03 of this code that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

Sect. 33.05. Assistance by Attorney General

The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation of prosecution of an offense under this chapter or of any other offense involving the use of a computer.

California Penal Code Section 502. Basic Computer Crime Statute

Section 502. [Computer crimes]

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means two or more computer systems connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.

(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access.

(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.

(c) Except as provided in subdivision (i), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses, or causes to be used, computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation which does not result in injury, and where the value of the computer services used does not exceed four hundred dollars ($400), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation which results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds four hundred dollars ($400), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6) or (7) of subdivision (c) is punishable as follows:

(A) For a first violation which does not result in injury, an infraction punishable by a fine not exceeding two hundred fifty dollars ($250).

(B) For any violation which results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation which results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the county jail not exceeding one year, or by both that fine and imprisonment.

(e) (1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.

(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees to a prevailing party.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) This section applies only to public offenses committed on or after January 1, 1988. It is the intent of the Legislature that this section be given no retroactive effect and persons who commit a violation of the provisions of Section 502 in effect prior to January 1, 1988, shall be held responsible therefor.

(h) Any computer, computer system, computer program, instrument, apparatus, device, plans, instructions, or written publication used in the commission of any public offense described in subdivision (c) may be seized under warrant or incident to a lawful arrest. Any property seized under this subdivision is subject to forfeiture pursuant to Section 502.01.

(i) (1) Subdivision (c) does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment.

(2) Paragraph (3) of subdivision (c) does not apply to any employee who accesses or uses his or her employer's computer system, computer network, computer program, or data when acting outside the scope of his or

her lawful employment, so long as the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or so long as the value of computer services, as defined in paragraph (4) of subdivision (b), which are used do not exceed one hundred dollars ($100).

(j) No activity exempted from prosecution under paragraph (2) of subdivision (i) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(k) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction for another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

Federal
Chapter XXI — Access Devices and Computers

Sec. 2101. This act may be cited as the "Computer Fraud and Abuse Act of 1986."

Sec. 2102. (a) Chapter 47 of title 18 of the United States Code as amended by chapter XVI of this joint resolution, is further amended by adding at the end thereof the following:

1030. Fraud and related activity in connection with computers

(a) Whoever—

"(1) knowingly accesses a computer without authorization, or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

"(2) intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

"(3) intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer; and

"(4) knowingly and without intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

"(5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—

"(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if —

"(A) such trafficking affects interstate or foreign commerce; or

"(B) such computer is used by or for the Government of the United States;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

"(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(1)(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which does not occur after a conviction for another offense punishable under this subparagraph; and

"(2)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

"(3)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph."

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

"(1) the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.";

"(2) the term 'Federal interest computer' means a computer—

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

"(B) which is one or two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term 'State' includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term 'financial institution' means—

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration

"(E) a member of the Federal home loan bank system and any home loan bank;

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; and

"(H) the Securities Investor Protection Corporation;

"(5) the term 'financial record' means information derived from any record held by a financial institution pertaining to a customer's relationship without the financial institution;

"(6) the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and

"(7) the term 'department of the United States' means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5."

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."

(g) The table of sections at the beginning of chapter 47 of title 18 of the United States Code is amended by adding at the end of the following new items: "1030. Fraud and related activity in connection with computers"

Sec. 2103 The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this joint resolution, concerning prosecutions under the sections of title 18 of the United States Code added by this chapter.

Note: The text of this section of title 18 was derived by SRI International on February 10, 1987, by applying the instructions for amendment found in Public Law 99-474 - Oct. 16, 1986 100STAT.1213. This amended version may be incorrectly produced, and readers are referred to the official title 18 text when it becomes available.

Federal
Chapter XVI. Credit Card Fraud

Sec. 1601. This chapter may be cited as the "Credit Card Fraud Act of 1984."

Sec. 1602. (a) Chapter 47 of title 18 of the United States Code is amended by adding at the end thereof the following:

1029. Fraud and related activity in connection with access devices

(a) Whoever—

"(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

"(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

"(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices; or

"(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b) (1) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) The punishment for an offense under subsection (a) or (b)(1) of this section is—

"(1) a fine of not more than the greater of $10,000 or twice the value obtained by the offense or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2) or (a)(3) of this section which does not occur after a conviction for another offense under either such subsection, or an attempt to commit an offense punishable under this paragraph:

"(2) a fine of not more than the greater of $50,000 or twice the value obtained by the offense or imprisonment for not more than fifteen years, or both, in the case of an offense under subsection (a)(1) or (a)(4) of this section which does not occur after a conviction for another offense under

either such subsection, or an attempt to commit an offense punishable under this paragraph; and

"(3) a fine of not more than the greater of $100,000 or twice the value obtained by the offense or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this paragraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

"(1) the term 'access device' means any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

"(2) the term 'counterfeit access device' means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

"(3) the term 'unauthorized access device' means any device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

"(4) the term 'produce' includes design, alter, authenticate, duplicate, or assemble;

"(5) the term 'traffic' means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of; and

"(6) the term 'device-making equipment' means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under title V of the Organized Crime Control Act of 1970 (18 U.S.C. note prec. 3481)."

(g) The table of sections at the beginning of chapter 47 of title 18 of the United States Code is amended by adding at the end the following new item:

"1029. Fraud and related activity in connection with access devices."

Sec. 1603. The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this Act, concerning prosecutions under the section of title 18 of the United States Code added by this chapter.

APPENDIX B

Citations of State Computer Crime Statutes

APPENDIX B: Citations of State Computer Crime Statutes

Appendix B*
State Computer Crime Statutes

Alabama—The Computer Crime Act punishes offenses against intellectual property—accessing, communication, examining, modifying, or destroying computer data without authorization. Unauthorized disclosure of data is a crime. Ala. Code 13A-8-101.

Alaska—"Property" in the criminal code includes "intangible personal property including data or information stored in a computer program, system, or network." Alaska Stat. sec. 11.81.900(b)(44).

Alas. Stat. sec. 11.46.200(a) was amended in 1984 to define the unauthorized use of computer time as "theft of services."

Arizona—State law defines types of crimes using computers and makes them punishable as felonies. Ariz. Rev. Stat. sec. 13-2301E. Also, 13-2316.

Arkansas—The Computer-Related Crimes Act of 1987 punishes offenses of computer fraud and computer trespass. It facilitates civil actions and provides for assistance from the state attorney general. Ark. Sec. 5-41-101 to 107.

California—It is a crime "to intentionally access . . . any computer system or computer network for the purpose of devising or executing any scheme or artifice; to defraud or extort or obtain money, property or services with false or fraudulent intent, representations, or promises; or to maliciously access, alter, delete, damage, or destroy, any computer system, computer network, computer program or data." Cal. Penal Code sec. 502.

Publishing a Personal Identification Number (PIN), password, access code, debt card number, or bank account number is a crime. Penal Code sec. 484j.

Colorado—This law, similar to Florida's, creates a Class 3 misdemeanor for computer crimes. Colo. Rev. Stat. sec. 18-5.5-101.

Connecticut—Computer crime is a misdemeanor or a felony, depending on the dollar amount involved. Conn. Gen. Stat. Ann. sec. 53a-250.

*Reprinted with permission from *Compilation of State and Federal Privacy Laws*, Privacy Journal, Washington, D.C. (1988).

Delaware—Accessing a computer system for defrauding or obtaining money or services is computer fraud, and intentionally accessing, altering, destroying or attempting to do so for an improper purpose is computer misuse, both felonies. Del. Code tit. 11, sec. 931 to 939.

Florida—It is a felony to commit offenses against intellectual property; against computer equipment or supplies; or against computer users. The law prohibits willful modification, destruction, and disclosure. Fla. Stat. Ann. sec. 815.01.

Georgia—Accessing or attempting to access a computer system owned by the state or under state contract or owned by any business is punishable by a fine and up to 15 years. Ga. Code Ann. sec. 16-9-90.

Hawaii—Computer fraud is a felony or misdemeanor depending upon the amount of money or damages involved. Computer fraud includes accessing a system with intent to defraud or to obtain money, get credit information, or introduce false information. Also, to wrongfully damage or enhance the credit rating of any person is a crime. Unauthorized computer use is a separate crime. Haw. Rev. Stat. 708-890.

Idaho—The law distinguishes between accessing or altering information with fraudulent purposes (a felony) and access only (a misdemeanor). Session Laws of Idaho 1984, ch. 68, p. 129, adding Idaho Code sec. 18-22.

Illinois—Without the consent of the owner, it is illegal to alter a computer program, to access a system, or to obtain uses or benefits from it. There is a civil right of action for victims of computer crime. Ill. Rev. Stat. Ann. ch. 38, sec. 16-9, as amended in 1983.

Indiana—A person who knowingly alters a computer program or data that is part of a system commits the felony of computer tampering. A person who accesses a system without consent commits a misdemeanor. IC 35-43-1-4.

Iowa—The computer crime law was effective July 1, 1984. Iowa Code Ann. sec. 716A.

Kansas—"Willfully exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing or taking possession ' are crimes, as well as using a computer to defraud or to obtain money fraudulently. Kans. Stat. sec. 21-3755.

Kentucky—Fraudulently accessing a system to defraud, to obtain money or services, or to alter, damage, or attempt

to alter information is a felony. Access for the sole purpose of obtaining information is a misdemeanor. A person is guilty of "misuse of computer information" when he or she receives, conceals, or uses any proceeds from an act in violation of the law (or aids another in doing so). Ch. 210, Acts of 1984, adding Ky Rev. Stat. sec. 434.

Louisiana—Computer-related offenses are defined in La. Rev. Stat. 14:73.1 through 5.

Maine—Rev. Stat. Ann. tit. 17-A, Sec. 357 (1964).

Maryland—"No person shall intentionally, willfully, and without authorization access, attempt to access, or cause access to a computer, computer network, computer software. . ." Personal home computers and dedicated computers are excluded. Md. Ann. Code Art. 27, sec. 146.

Massachusetts—"Property" in the larceny statute includes "electronically processed or stored data, either tangible or intangible [and] data while in transit." Mass. Gen. Laws Ann. ch. 266, sec. 30(2).

Michigan—Computer fraud is a crime. Mich. Comp. Laws Ann. sec. 752.791.

Minnesota—Whoever intentionally and without authority damages or alters computer media is subject to a fine, depending on the loss involved, and prison term. Minn. Stat. Ann. sec. 609.87.

Mississippi—Computer fraud is a crime, as well as intentionally denying an authorized user effective use of a system or disclosure or misuse of codes or passwords. Miss. Code Ann. sec. 97-45-1.

Missouri—It is a crime to tamper with intellectual property. Mo. Ann. Stat. sec. 569.093.

Montana—The criminal code prohibits unlawful use of a computer, and "property" as defined in the criminal code on theft includes "any tangible or intangible thing of value . . . electronic impulses, electronically processed or produced data." Mont. Code Ann. 45-6-310.

Nebraska—Unauthorized access or disruption of a computer system is a felony. Neb. Rev. Stat. sec. 28-1343.

Nevada—A person who without authority denies the use of a computer to a person who has the duty and the right to use it is guilty of a misdemeanor. Also, using a computer without authority, to get personal information on another or to enter false information about another person in order to alter a credit rating is a crime. Nev. Rev. Stat. sec. 205.473.

New Hampshire—Accessing, intercepting, or adding to computer data is a crime, unless the person believed that he had authority. N.H. Rev. Stat. Ann. sec. 638:16.

New Jersey—There is a civil liability for computer-related fraud (NJ. Rev. Stat. sec. 2A:38A-1) and criminal liability (NJ. Rev. Stat. sec. 2C:20-1).

New Mexico—Misuse of a computer is a felony. Computer Crimes Act of 1979. N.M. Stat. Ann. sec. 30-16A-1.

New York—Intruding into a computer system with confidential medical or personal information is a crime. Also, tampering with computer data while trying to commit a felony is itself an offense, as well as making unauthorized duplications of data. The law permits the state to prosecute a person in another state who taps into a computer in New York without authorization. N.Y. Penal Law Art. 156.

North Carolina—This law punishes computer-related offenses, including physical damage to a unit, wrongfully accessing a computer or network, and altering or damaging computer software, and seeking to extort by use of a computer. N.C. Gen. Stat. 14-453.

North Dakota—Computer fraud by accessing, altering, damaging, destroying without authority with intent to defraud or deceive or control property or services is a Class B felony. Doing so without false pretense is a Class C felony. N.D. Cent. Code sec. 12.1-06.1-08.

Ohio—The criminal code was amended in 1982 to include computer media in the definition of stolen property. Ohio Rev. Code Ann. sec. 2901.01 and 2913.01.

Oklahoma—Like Pennsylvania's, this law, passed in 1984, distinguishes computer hacking (a misdemeanor) from fraudulent alteration of, or damage to, computer data (a felony). Okla. Stat. Ann. tit. 21, sec. 1951-1956.

Oregon—Two classes of computer fraud are defined, prohibiting unauthorized access to systems. Or. Rev. Stat. 164.277.

Pennsylvania—Accessing, altering, damaging, or destroying any computer, system, or data base with criminal intent is a third-degree felony. Tampering, where no greater crime occurs, is a misdemeanor. Pa. Stat. Ann. tit. 18, sec. 3933.

Rhode Island—Similar to California's law, R.I. Gen. Laws sec. 11-52-1.

South Carolina—The computer crime law defines "computer hacking." S.C. Code sec. 16-16-10.

South Dakota—The state's 1982 law was amended in 1984 to punish "computer hacking," including the use or disclosure of passwords without the consent of the owner. It also punishes wrongful access to computerized information, as well as altering or disclosing. S.D. Codified Laws Ann. sec. 43-43B-7.

Tennessee—The Computer Crimes Act of 1983 prohibits damaging or altering computers or computer data. Tenn. Code Ann. sec. 39-3-1404.

Texas—It is a misdemeanor to use a computer or to gain access to it without consent when there is a computer security system in place; or to alter or damage a program or cause a system to malfunction. It is a felony if the loss exceeds $2,500. Tex. Penal Code Ann. 33.01. It is a misdemeanor to disclose a secure password to another person. Legislative records are protected by Tex. Civ. Stat. Ann. art. 5429b.

Utah—The altering, damaging or wrongful access of computer records is punishable as a misdemeanor or felony. Utah Code Ann. sec. 76-6-701.

Virginia—Fraudulent use of a system as well as trespassing in a system so as to cause a malfunction, alter data, or affect a financial transaction, is prohibited. It is a crime to invade one's privacy by perusing medical, employment, salary, credit, or other financial or personal data relating to another person and stored in a computer. Va. Code Ann. sec. 18.2-152.1, enacted in April 1984.

Washington—The computer crime law was enacted in March 1984. Wash. Rev. Code Ann. sec. 9A.48.100.

Wisconsin—It is a crime to modify, destroy, access, take, or copy data, programs, or supporting documentation in a computer. Wisc. Stat. Ann. sec. 943.70.

Wyoming—Passed in 1982 and amended the next year, the law defines crimes against intellectual property and makes it a crime wrongfully to access a system or to deny computer services to an authorized user. Another section prohibits crimes against equipment, including impairing government or public services. And a third section defines crimes against computer users. Wyo. Stat. sec. 6-3-501 through 504.

APPENDIX C

Selected Cases Reported in the News Media

APPENDIX C: Selected Cases Reported in the News Media

Introduction

To supplement the meager documentation on computer crime, this appendix briefly describes a few of the 3,000 cases in the SRI International computer abuse file in which legal action took place and which were reported in the news media. The cases presented are not meant to be representative, nor necessarily entirely accurate (because of their source), but to provide a starting point for prosecutors confronted with similar facts.

The number preceding the case title identifies the case. The first two digits correspond to the year the crime was perpetrated. The third digit indicates its type as follows:

(2) Intellectual property—deception or taking

(3) Financial data—deception or taking

(4) Unauthorized use of services.

The last digit (or last two digits) indicate the order in which cases were discovered. The reviewer's comments and primary source follow each case description. Cases are in order by type and year within type.

Case Descriptions

72219 Software Acquired by Man Posing as Professor

In 1972, the soon-to-be operator of a Paris software house raided more than 100 U.S. industrial, public utility, banking, and retail computer centers and succeeded in bilking them out of most of their confidential programs. He did this by first posing as a professor of computer science and offering to give a series of 13 lectures at a French university at no cost. He gave the first six lectures and then disappeared with a supply of the university's letterhead. He then wrote to the computer centers of more than 200 U.S. companies, asking for permission to visit to learn about programming and software technology. He said that the information he gained would be used for teaching purposes only. Replies were to be sent to him care of the French university.

More than 100 companies welcomed him, gave him virtually free run of their computer centers, copies of their programs, and some even paid his hotel expenses. None of them checked his credentials. He acquired so many program tapes that he had to take a freighter home. There he began a software mail order business in his home. In 6 months, he had netted more than $80,000 and was employing nine people.

A midwestern flour milling company discovered he was selling copies of one of their top secret computer programs (one they had not given him; the suspect bribed a staff member for it). The firm lodged a complaint with French authorities who raided the suspect's headquarters and seized all the tapes. He pleaded guilty to dealing in stolen property and paid about a 5,000 franc fine. All the tapes, except that of the flour milling company, were returned to him.

He has since moved his operation to Italy and expanded his sales to Japan, Australia, the Middle East, Eastern bloc countries, and Red China, as well as Western Europe. In 1974, he opened a branch in Argentina.

Reviewer's comments:

Impersonation, misrepresentation, unauthorized copying.

Source:

Farr, Robert, *The Electronic Criminals*, 2 January 1975

74223 Software Trade Secrets Violation

A Big Eight accounting firm was accused by another company of stealing trade secrets and reproducing software that it developed. The Big Eight accounting firm was charged and found guilty of selling PRIDE, a systems program, to a motorcycle manufacturer. The software developer was invited to demonstrate its product at a sales meeting at the manufacturer's offices and was joined by members of the accounting firm. The software developer claims that the secrets were revealed during this meeting and that the accounting firm representatives had also broken a nondisclosure agreement signed at that meeting.

In court, witnesses said that the information found in the program is found in the professional literature and that an experienced systems designer could duplicate the system in 2,500 hours. The basis for the accounting firm's defense was that the developer put a copyright notation on all its documents. Once an inventor has claimed the benefits of copyrighting, he is no longer protected by the trade secrets law.

At this point, the case went back for appeal. Both parties have admitted that it is a matter of principle that has run into more than $1.5 million in court fees.

Reviewer's comments:

This case is one of a series involving interpretation of copyright protection for software products.

Sources:

Information Systems News, 21 April 1980

75204 Oil Theft from a Refinery

Thirteen defendants were arrested in New Jersey in March 1975 on a variety of charges, including larceny, fraud, conspiracy, and receiving stolen property. The case involved theft of nearly 16 million gallons of home heating oil from an oil refinery between March 1969 and March 1975. The value of the loss was estimated to be $4.3 million.

A suspect and his son (a former state senator) were indicted on 317 counts. Other defendants who pleaded guilty testified that the father and son had masterminded the scheme. The captain of their oil tanker (and for a short time, his predecessor) arranged with two oil company tank gaugers, an oil company computer operator, and an oil company dock worker to falsify the gauge readings, computer records, invoices, loading slips, and other documents.

Typically, the tanker was authorized to pick up 2,000 gallons of heating oil per trip for the ring leaders' companies. In fact, the ship would be filled to its 4,000-gallon capacity, but the gauge rigged to show only 2,000 gallons.

An oil company spokesman indicated that the refinery has hundreds of storage tanks with capacities ranging from 1,680,000 to 6,300,000 gallons at the refinery. The amount that could not be accounted for was hard to detect, and within the percentage of losses anticipated by giant corporations.

On an informant's tip, the oil company notified authorities who arrested the employees on March 19, 1985. The tanker filled to capacity, was also seized. Subsequently, most of the defendants pleaded guilty and received fines and suspended sentences. The captain was tried, found guilty, and sentenced to 3 years. Both the father and the son were convicted. The son was sentenced to 9 years and a $51,000 fine, the father to 12 years and a $203,000 fine (the maximum fine possible). They appealed the decision. The oil company has also instituted a $3.4 million civil suit against the father and son, and smaller suits against the other defendants. The civil suits were deferred pending the outcome of the criminal cases because of the requirements for disclosure in civil cases.

Reviewer's comments:

Collusion, false data entry, rigging

Sources:

NY Times, 20 March 1975
Daily Journal, Elizabeth, NJ; 20 March 1975, 2 April 1975, 9 October 1975, and 22 January 1977
Courier News, Plainfield, NJ; 25 November 1975

78216 Theft of Pharmaceuticals

The accused, age 34, systematically robbed his employer, a major pharmaceutical company, of $1.3 million worth of over-the-counter products over a 7-year period. He began his thefts while a computer programmer at one of the firm's distribution plants in Massachusetts and continued when he was promoted to computer operations manager at a New Jersey distribution center until his activities were discovered and he was fired in 1978.

The accused concealed the thefts by billing house accounts used for exchanges and samples. In some instances, he transmitted false invoices from New Jersey to Massachusetts, waited until he was sure the dispatch note had been generated, then destroyed the invoice in New Jersey so that there would be no record of the transaction. Some products he used himself; most he sold to a fence to support his $700 a week drug habit.

He was convicted of five counts of wire fraud in New Jersey and sentenced to 3 years in prison.
Reviewer's comments:

Unauthorized use, false data entry, embezzlement. Better separation of duties and better auditing controls could have prevented this crime or detected it earlier.

Sources:

Boston Globe, 23 February 1980
Star Ledger, Newark, NJ; 23 February 1980, 30 April 1980, and 10 June 1980
Computerworld, 17 March 1980 and 5 May 1980

78219 Trade Secret Violation

The accused, age 42, was convicted of possessing proprietary chip designs (worth as much as $10 million) belonging to three major semiconductor firms. The case holds particular legal significance because when the accused and two codefendants were indicted in November 1978 and charged with theft, possession of stolen property, conspiracy, bribery, and solicitation, a judge of the Santa Clara County Superior Court suppressed 95% of the evidence in the case. Until this decision was reversed by the State Appeals Court Panel, it appeared that the case would have to be dropped for lack of admissible evidence.

At issue was the manner in which the evidence was seized. When police went to the accused's business, they had

a proper search warrant spelling out precisely the items for which they were searching. However, the officers themselves did not perform the search. Because the technical nature of the items involved was considerably more complex than laymen could understand and identify, employees of two of the victimized firms accompanied the police to identify the items in the warrant. The appeals court opinion said the use of experts was analogous to police use of dogs to sniff out marijuana. "We think there is no requirement that such experts, prior to stating their conclusions, engage in the futile task of attempting to educate accompanying police."

The case also has special significance according to the deputy district attorney for Santa Clara County, because it is believed to be the first criminal case in which integrated circuits were held to be trade secrets. This could be interpreted as outlawing the practice of reverse engineering (buying and copying an integrated circuit design).

Although not an issue during the trial, authorities claim to have linked the accused (originally from Singapore) to Soviet Bloc countries. Business cards of Soviet and Polish technology procurement officers were found in his offices.

Reviewer's comments:

Espionage, unauthorized copying of circuit designs

Sources:

Peninsula Times Tribune, Palo Alto, California; 2 May 1980
Wall Street Journal, 15 July 1981
Computerworld, 20 July 1981
Memorandum from Samuel Hoar, 13 August 1981

80209 Computer Used to Embezzle Payroll Funds

A federal agency employee, formerly a clerk in charge of its payroll, was indicted for mail fraud, conversion of government property, false claims, aiding and abetting, and embezzlement, among 54 counts. He was accused of using his position in which he prepared batch materials for computer processing on the 1,400-person payroll and corrected erroneous payroll transactions from computer edit reports to issue checks to at least six ineligible individuals. The checks, according to one source, totalled as much as $45,000. The clerk allegedly split the money with the individuals to whom the checks were written.

The fraud was discovered when agency officials noted that checks had been written to individuals who were not employed by the agency. The fraud had evidently begun in September 1979. The clerk was arrested on February 1, 1980. All five of the alleged recipients pleaded guilty to various charges in connection with the case.

Reviewer's comments:

False data entry by an authorized user.

Sources:

Washington Post, 20 February 1930
Washington Star, 18 March 1980
Computerworld, 3 March 1980

84210 Ex-Employee Steals Licensed Source Code from Former Employer

A former computer company employee was discovered stealing licensed source code after he bluffed his way back into a computer center. The police report says he entered the building, flashed his old badge, but signed in using the name of another employee. An employee working that night noticed the computer activity and sent computer messages to the suspect asking for his identification. The suspect called the employee and identified himself as the employee he had signed in as. The employee recognized the suspect's voice and alerted security guards, who confiscated tapes containing source code and ejected the suspect from the premises.

According to police, the suspect allegedly stole three computer tapes from his old employer's corporate offices 2 days before he joined a small software firm. The suspect intended to run the tapes on his new employer's hardware, but found that the tapes were incompatible with its system. On 21 June 1984 he entered the old company, attempted to reformat tapes, but was discovered. The incident prompted a 3-month investigation, which led to the suspect surrendering to police on 14 September 1984. The suspect was charged with five felonies, including two counts of computer crime, one count of stealing trade secrets, and two counts of burglary. He was released on $10,000 bail.

Reviewer's comments:

This case is an example of a talented employee attempting to make points with a new employer by supplying pirated software. The new employer should have fired this person at the first hint of such activity.

Sources:

Peninsula Times Tribune, Palo Alto, California; September 1984
Computerworld, 1 October 1984

85217 Company Changes Records in Regional Credit Bureau Files

An international firm arranged excellent credit ratings for poor credit risks by damaging, destroying, or otherwise manipulating the credit files of clients who paid it large cash fees (the initial payment was often $1,500). The firm would

access the confidential files of the regional credit bureau until it found a target individual, somebody with sterling credit ratings and an identity similar to that of its client. The client actually assumed the target's identity, using his name, address, and details of family life in securing a loan or a credit card. In other cases, the company fixed the master computer records so that damaging data on its client could not be extracted.

Reviewer's comments:

Apparently, the regional credit bureau not only permitted easy access to its files, but also had insufficiently protected data records. In a case like this, read-only privileges should have been granted, if that. The fact that this crime could be committed with a home computer and a modem does not speak well for the credit bureau. Area merchants who lost heavily could probably have brought negligence charges against the credit bureau.

Since the firm engaged in long-term, undetected access, this case represents impersonation of legitimate users rather than bypass of controls, modification, or direct misuse.

Sources:

Texas Business, April 1985

85220 Software Piracy—Unauthorized Copying of Database System

A former data processing manager alleged to the FBI that a research institute made and distributed an unauthorized copy of a proprietary software package. The illegal copy was provided to a New York typesetting firm.

The developer entered a $3 million lawsuit against the institute and its president, as well as the receiver of the software and its president. In addition to the illegal copying of the software package, FBI agents also found some illegal copies of another program. Of concern to the FBI were violations of copyright statutes under Title 17 of the Federal Rules of Criminal Procedure and interstate transportation of stolen property.

Reviewer's comments:

This case is important because it is believed to be the first formal federal probe of a software piracy case. The techniques employed, of course, were elementary copying of software.

Sources:

Edpacs, November 1985
Computerworld, 14 October 1985

86236 Data Capture Operator Took Advantage of System Weakness

A data capture clerk for a small component manufacturing company conspired with a customer to defraud the company. The customer would return goods and the clerk would enter a larger quantity of goods returned than were actually brought back to the store.

The fraud was discovered in May 1984 when the dispatch manager investigated and found the falsification. Subsequently, a consultant was hired and the full extent of the fraud was discovered. Although neither the clerk nor the customer were prosecuted, the company improved its manual system, setting up a direct feed between manual processes and the computer operations.

Reviewer's comments:

False data entry

Sources:

Aiken & Carter, "Computer Crime in South Africa," 1986, page 32.

88214 Data Destruction and Logic Bomb Case

The victim company involved in this case is a licensed life insurance agency and registered securities dealership. Independent agents make sales for this company, and the agents are paid a commission based on their sales. At the time of the offense, commission payments averaged two million dollars a month to approximately 450 independent agents.

Most of the commissions are calculated from records on magnetic tapes submitted monthly by insurance and securities firms across the country. The company's mainframe computer processes these tapes and produces commission reports on a monthly basis. This computer process includes the creation of three commission "detail files" and a commission "master file."

It was discovered one morning that the computer system had suffered a major loss of records from the detail files. More specifically, over 160,000 records had been deleted from each of the three files, amounting to about 75% of each file. Without these records, the monthly commission report could not be created, and the independent agents could not be paid.

Through the history log on the system, the deletions were linked to system access that had occurred between 3 a.m. and 3:30 a.m. earlier that morning. Someone had used the system then to run a series of programs that resulted in the

deletions of the records. Further investigation determined that these programs had been created approximately three weeks prior.

Three days before this incident, a senior systems analyst had been involuntarily terminated from the company. The analyst, who had been with the company for two years, was the operations manager and the company's computer security officer. After an initial investigation by the company, the former employee was determined to be the prime suspect. The company sued in Civil Court for illegal trespass, breach of fiduciary duty, and gross negligence. The jury agreed with the company and ordered the defendant to pay approximately $12,000 in damages.

The defendant was then charged in criminal court with burglary, harmful access to a computer with loss and damages over $2,500 (a felony offense in this state), and criminal mischief over $750. The case proceeded to a jury trial that lasted two weeks. The defendant was found guilty by the jury. He was ordered to pay $11,800 in restitution to the company and sentenced to 7 years of supervised probation.

The head of the county's computer crime unit was the prosecutor in this case. His extensive knowledge of computers and the state's computer law was very beneficial in the successful prosecution. The defendant hired defense attorneys who were also very knowledgeable about computers. In response to the criminal charges, the defense eventually filed 30 motions, including 13 discovery motions, three motions relating to challenges to the indictment, and three motions to dismiss related to destruction of evidence.

Like many internal computer crime cases, there were many complexities in this case. For example, anyone wanting to access the mainframe computer had to "sign on" from a terminal. The sign-on procedure required the person to first enter into the terminal an account name identifying the user. Then, a password uniquely associated with the account name had to be provided. Access was denied if someone attempted to use a valid password from another account name.

On the day that the defendant was terminated from the company, his account was removed from the computer system and a new password for the security officer was created. It is believed that the defendant reentered the building three days after being fired and accessed the computer using an account name he created prior to his termination. This account name was probably created for the specific purpose of allowing him access in the event he was terminated or quit. He then ran the security functions program which provided the security functions menu and the new security officer's password. With this information, he could bypass the security mechanism and obtain complete access to the system. A series of programs were then run which resulted in the destruction of the records in the three data files.

As part of the procedure, these programs were copied and given new names, and the old versions of the programs were deleted. Further, each destructive program read a data area to determine (1) the date that the deletion and copy programs should run next and (2) the current names of the programs. This overall procedure would be activated by the programs creating the commission detail records and would result in the deletion of files on a monthly basis. It would also make the tracing of the deletions more difficult in the future. Fortunately, this procedure was found before it could be activated.

Reviewer's comments:

When it was discovered that there had been a major loss of records, the entire system was copied to 12 magnetic tapes. This step allowed analysis at a later date on exactly what was on the system at the time of the loss.

One defense motion requested the use of the victim's computer to examine the backup tapes. Obviously, the company objected strongly to this request. While the motion was being considered, the state and the defense reached an agreement allowing the defense access to the tapes over one weekend on a computer system provided by the defendant. Further, the company controlled the loading of the tapes and the access to the information. All printed materials stayed in the possession of the state until released by agreement or by court order.

Sources:

Dedicated Computer Crime Units. J. Thomas McEwen, National Institute of Justice (1989).

75335 Programmer "Sliced Off" Fractional Shares in Investment Plan and Put Them in Own Account

In this salami swindle a programmer sliced off rather than rounded off fractional shares employees bought in their employee investment plan and transferred those fractions to his own account. When he was caught, he had credited his account with about $380,000 worth of securities.

Reviewer's comments:

This case is a known example of a salami swindle.

Sources:

Computerworld, 3 December 1975

75344 Medi-Cal Fraud (Physicians)

A management consultant was retained by six Oakland, California, physicians to obtain back medical billings from Medi-Cal. He received from 25% to 28% of the face value of the claim processed as his fee. The consultant discovered through acquaintances in Medi-Cal's processing agent, and by examining computer manuals, that the computer did not

check claims more than one year old as possible duplicates. He met with a claims supervisor who agreed to help him process the duplicate claims using a computer override and "not late" stamps on the claims, and then entering a code on the claim that would override the system's safeguards.

In 1974 and 1975, they processed 447 claims totaling $33,123.20 according to one report. The operation was discovered as a result of hearings conducted by the Little Hoover Commission investigating fiscal management in the California Department of Health. They interrogated the consultant, who confessed and implicated the supervisor. He then cooperated with investigators, giving the supervisor $13,000 in marked duplicate claims, which she processed. Their meetings and actions were monitored and recorded by Department of Justice agents. When arrested, the supervisor also confessed. In November 1976, both received suspended sentences.

Reviewer's comments:

The amount was probably more than $33,000. The case involved false data entry and collusion.

Sources:

Oakland Tribune, 20 March 1977
Edelhertz, Herbert, *The Investigation of White Collar Crime*, May 1977

78303 Checks Issued on Reactivated LA Welfare Cases

The accused, age 30, was hired by a county Department of Public Social Services (DPSS) in June 1975. In January 1978, he offered to help a couple who told him they were having financial difficulties. He put the couple on the welfare rolls and, as a result, they received $10,757 between January 9, 1978, and March 4, 1978 (a feature of the computer system allowed recipients to receive as much as 6 months back payment once aid was approved). According to their testimony, they gave the accused half of that amount for helping them.

The accused had entered the case as if it had come from a different branch office. Employees there could not match it to any of their case files and forwarded it to another office with the same result. DPSS investigators identified and questioned the couple who then implicated the accused. Investigators also discovered that the accused had stolen much more. He was charged with grand theft (1 count) and theft of public funds (11 counts) in that amount. He pleaded not guilty. After the preliminary hearing, he jumped bail. Final disposition of the case is not indicated in the file.

Reviewer's comments:

Unauthorized use, false data entry, collusion, embezzlement

Sources:

State of California, County of Los Angeles, Docket # A342 572 reports (undated)
Defendant, affidavit, 9 March 78
Computerworld, 29 May 1978
Cancelled checks and welfare office documents

78310 Withdrawal of $927,000 Deposited through a Keypunch Error

A bank clerk made a one-digit error in a bank transfer posting that resulted in $927,288 belonging to a commercial account being deposited to the account of the accused, age 52, a bookkeeper. When the accused received his June 1978 bank statement, he began to withdraw the money systematically. He wrote checks to 10 to 15 people and apparently retrieved the proceeds from them. He left town on August 10, the day the bank, investigating the commercial client's inquiry about its deposit, traced it to the accused's account. A warrant was issued for his arrest.

He was presumed to have fled to Florida with his wife. On September 8 he surrendered at the U.S. marshall's office. He said he had just returned from "a long-planned vacation in Europe." He was indicted, pleaded innocent, and was held on $100,000 bail.

Between August 10 and September 8, the accused had flown to Stockholm by way of Copenhagen and Helsinki, laundering the funds in a series of transactions between European, American, and Canadian banks. Somewhat less than $300,000 was accounted for, and very little of that recovered as of October 1978. Authorities were able to trace approximately $150,000 to monies used to pay mortgages and liens on properties owned by companies in which the accused had an interest, $100,000 was used to pay a debt to a business associate, and $38,000 purchased stock in Western Empire Corp., giving the accused a controlling interest.

Reviewer's comments:

Data entry error, withdrawal of funds erroneously deposited to another's account, fugitive from justice, concealment of funds, felony theft.

Sources:

Los Angeles Times, 16 August 1978, 17 August 1978, and 22 September 1978
American Banker, 18 August 1978
Computerworld, 2 October 1978

78313 $10.2 Million Transfer

On October 25, 1978, the defendant (with a master's degree in computer science from UCLA) used inside knowledge of a major bank's code of the day to transfer

$10.2 million from the general funds of a control account from a Los Angeles branch to his own private account in New York City by impersonating a bank official. He subsequently transferred most of that money to the Swiss bank account of Russalmaz (the official diamond broker of the Soviet government), flew to Zurich, and returned with $8.1 million in small polished diamonds. He had physical access to the bank's wire fund transfer facilities because he was known to have worked as a consultant to install an emergency backup wire transfer system. The code of the day had been in plain view when he entered the wire transfer room, ostensibly to do a performance evaluation on the primary system. He was convicted in 1979 and served 3 years in California's Lompoc Federal Prison Camp.

Side note: He had considered a Trojan horse trap door attack on the computer system, but decided that the "confidence" access was less risky.

Reviewer's comments:

The illegal wire transfer, with resulting loss of $2.8 million after recovery and auction of the gems, could have been avoided by simple security measures—requiring proper identification before admittance and restricting knowledge of the code of the day to authorized employees.

Sources:

Bruce Henderson and Jeffrey Young, "The Heist," *Esquire*, pp 36-47 (May 1981).
Donn Parker and Susan Nycum, Interview with Robin Brown, FBI, Los Angeles (13 May 1981)
San Jose Mercury News, San Jose, CA; 16 November 1978
Wall Street Journal, 7 November 1978

78324 Retirement System Fraud

Sloppy bookkeeping and a total lack of computer security procedures enabled a supervisor and two clerks in the refund section of a state Supplemental Retirement System (SRS) to embezzle $111,249.56. The SRS served 230,000 state and local government employees and public school teachers and had over $1.3 billion in assets. The thefts, although crude, were not discovered until 1978 when the State Auditor of Public Accounts conducted the first audit in 5 years. Among other serious deficiencies in its operations, the audit uncovered the scheme in which 29 fraudulent accounts were created on the computer and money withdrawn from them, 12 inactive members' accounts looted, vouchers altered, and fraudulent vouchers created. This took place over a 14-month period between November 12, 1976 and January 17, 1978.

The refund section supervisor, and two former clerks, were indicted for embezzling funds by filing false vouchers, causing payment checks to be issued to their addresses and those of family and friends, with whom they split the proceeds. In all, 17 individuals were indicted. One was out of state and not arrested at the time of the cited sources. One was found innocent. The rest were either convicted or pleaded guilty.

The supervisor was sentenced to 8 years, the clerks to 6 years. The rest received various sentences—some prison terms, some suspended, some fined, some ordered to make restitution, or a combination of the above.

Reviewer's comments:

Collusion, false data entry, embezzlement

Sources:

Richmond News Leader, 23 March 1978, 2 May 1978, 20 July 1978, and 11 October 1978

83319 $1.7 Million Jackpot Slot Machine Scam

On August 15, 1983, a progressive 5-slot machine payoff of $1.7 million was externally triggered. Although the casino's officials have attempted to keep the details quiet, apparently a battery-powered "black box" microprocessor was plugged into the "data socket" used for test purposes, the voltage was overloaded, and the slot machine was controlled from the external microprocessor.

This remarkable case involved a confluence of high-tech attacks and considerable inside knowledge about both the hardware and software of the slot machine and the operations of the casino. A 19-count indictment was filed against 11 people (not including the actual "winner," who was apparently given immunity in exchange for his testimony). This group was implicated in 17 separate slot machine rigging incidents in three years, with the other cases totaling an additional $1.5 million.

Reviewer's comments:

Apparently, organized crime has gone high tech.

Sources:

Seattle Times, Seattle, WA; 22 September 1983.
Sun, Las Vegas, NV; 16 September 1983.
Nevada State Journal, Reno, NV; 21 September 1983.
Computerworld, 30 July 1984.

84306 Unauthorized Access and Modification of Data to Issue Fraudulent Checks

A clerk in a federal agency's financial management division was arrested on 25 October 1984 and charged with accessing a government computer and modifying data without proper authorization. Between August and October, the clerk and three cohorts had cashed more than 40

fraudulent checks worth approximately $160,000. The clerk apparently was the first person indicted under a federal law prohibiting unauthorized entry into government computers. The four suspects also faced charges of attempting to file a false claim with the U.S. government, defrauding the government and embezzlement.

Reviewer's comments:

> The software used had improper accounting controls/checks and balances. Questions still remain as to whether other checks were issued to other individuals and not detected. Basically, it is a case of false data entry.

Sources:

Recorder, San Francisco, CA; 15 November 1984
Computerworld, 3 December 1984
EDPACS, December 1984

84417 Four Youths Break into Unclassified Computers

Four hackers broke into two mainframe computers at a federal agency after discovering the computers' telephone numbers by scanning telephone lines. The newspaper accounts of the incidents did not directly indicate how the password and access codes were determined, but did say the hackers followed techniques used in the movie "War Games." The equipment used by the hackers included: IBM PCs, Apple II, Commodore 64, and autodial modems.

One newspaper article reported that agency officials said they were tipped off to the intrusion from its start on 28 June 1984 by "automatic systems." Later, the hackers left messages on the systems: "You can't catch me," "To be a nice boy, stop before I get angry," and "I think it is clear by now that you are up against some of the best hackers in the Huntsville area." Other articles stated the messages were the first indication that the agency's system had been penetrated. The hackers also deleted entries from the system log-on that logged their activity on the system.

The agency notified the FBI on 28 June 1984 but it took about 10 days to trace the calls. The FBI raided the homes of the four suspected hackers after calling their homes and posing as surveyers to verify the homes had PCs and user-developed software.

Reviewer's comments:

> This case illustrates the influence of movies on young people.

Sources:

News-Sentinel, Knoxville, TN; 17 July 1984
Huntsville News, Huntsville, AL; 18 July 1984
Union Leader, Manchester, NH; 18 July 1984
Post-Herald, Birmingham, AL; 18 July 1984
Huntsville Times, Huntsville, AL; 17 July 1984 and 24 July 1984
Computerworld, 27 August 1984 and 29 October 1984

85401 Hacker Accessed U.S. Forest Service Computer

A Los Angeles computer operator used a communications network to access computers illegally at a federal agency's regional offices. The defendant allegedly dialed into the network, inserted false user codes and passwords into the computer programs, and made printouts of information from the computer files. The defendant tapped the line of a Los Angeles optometrist, a network subscriber who was getting unexplained charges on his telephone bills. The trespass was first discovered by the director of quality assurance at the communications company in Virginia. He happened to be monitoring the network at home on his computer.

The defendant was indicted under the then-new Computer Fraud and Abuse Act. The indictment contained seven charges, which included four misdemeanor charges brought under the law against breaking into federal computers, two counts of felony wire fraud, and one felony count for making false statements to a federal agency. The charges covered a period from December 22, 1984 through January 26, 1985. Three of the felony charges were dropped in a plea bargaining process with prosecutors. "The misdemeanor charges are significant because we wanted to get some convictions under the new law," said an assistant U.S. attorney. Under the plea bargaining the defendant forfeited his computer equipment, which was seized on his arrest, and had to issue a statement explaining how he committed the offenses.

The defendant claimed that he did not think he was trespassing because he was still in his own home. He complained that the computer programs did not have notices warning against trespassing.

Reviewer's comments:

> This is a milestone case of the 1984 Computer Fraud and Abuse Act. It illustrates many hacking and phreaking techniques and excuses.

Sources:

Computerworld, 24 June 1985, p. 26
Computerworld, 11 February 1985, p. 2
Computerworld, 27 May 1985, p. 2
Herald Examiner, Los Angeles; 16 June 1985
Online Today, 17 May 1985, p. OLT-657
Post, Washington, D.C., 7 February 1985

85465 Unauthorized Use of Several Computers in Seattle Area

An 18-year-old computer wizard carried out hacking attacks against four major Seattle area firms and engaged in various other criminal activities in the fall of 1985 and early part of 1986. The suspect used a modem and several stolen PCs to carry out his attacks on companies with VAX systems. After using a telephone scanning device to locate computer tones, he determined if the target system was a VAX system. If it was a VAX system, he used SYSTEST and FIELD, which were standard default passwords shipped with VAXs from DEC, to attempt to break into the systems. These passwords were supposed to be removed after a system becomes operational, but DEC maintenance personnel used them when they would work on systems. Once into a system, the suspect could give himself superuser privileges, with the power to copy, destroy, or alter sensitive data. In one case, the suspect constructed the hacker's equivalent of the atom bomb—a package of global delete commands with subroutines labeled with titles like "Good," "Power," and "Zap."

Because the suspect could quickly penetrate these systems with SYSTEST and FIELD, he was not detected by the usual lengthy attempts at finding a valid password. The data processing manager at one company had written a program that constantly scanned the accounting facility in VMS, the operating system of the DEC VAX minicomputer that each of the victimized companies used. The program generates a report on calls that come in through the VAX's modem ports; the suspect's penetration was not detected because he made far fewer than the typical 5000 attempts to guess a password. Eventually though, someone realized that the DEC service accounts were being used late in the evening. The data processing manager went to his superiors to gain permission to try to catch the hacker. A phone-line tap was arranged to trace the calls. That trace led to the apartment of a drug dealer who had taken in the suspect after meeting him in Hawaii. The police confiscated four personal computers (three of which were stolen from the University of North Dakota), several hundred floppy disks, stacks of printouts, computer manuals, and notes written by the suspect. Drug paraphernalia were also found. The suspect was also believed to be involved in credit card fraud and phone phreaking.

Reviewer's comments:

This was an external attack.

Sources:

InformationWEEK, 21 April 1986, p. 30
Seattle P.I., 20 February 1986, 7 May 1986
Seattle Times, 28 February 1986, 7 May 1986
Bellevue Journal, 21 February 1986, 28 February 1986, and 7 May 1986

APPENDIX D

Data Processing Occupations and Their Risks in Computer Technology

best copy available

APPENDIX D: Data Processing Occupations and Their Risks in Computer Technology

Seventeen occupations in computer technology are described here in terms of their skills, knowledge, and access to do harm and cause loss. These occupational descriptions also apply to managers of people in these occupations who have the same capabilities as their employees. Note, however, that non-data processing occupations that are not discussed can also involve risks to computers and data. Computers—and especially microcomputers, in many cases accessing mini- and mainframe computers—are proliferating throughout information-intensive organizations and throughout society. Therefore, many types of people have the potential for engaging in computer crime.

User Transaction and Data Entry Operator

Function. Operates a remote terminal, enters transactions, data, and programs, at the direction of user personnel.

Knowledge. Source document content and format, terminal output content and format, terminal protocol, identification/verification procedure, other procedural controls, and possible vulnerabilities in access controls.

Skills. Typing and keyboard operation, manual dexterity for equipment operation, basic reading.

Access. Terminal area, source documents, terminal output, terminal operation instructions, identification/verification materials.

Vulnerability. The enterprise is vulnerable to both physical and operational violations by this individual. The principal area of vulnerability is violations that involve loss of the integrity, confidentiality, and availability of data belonging to the individual's immediate user organization either internal or external to the system. Two secondary areas of vulnerability are the unavailability or loss of confidentiality of the user organization's application programs either internal or external to the system and the physical destruction or taking of terminal equipment.

Conclusions. This individual is in a key position relative to the immediate user organization's data and programs entering the system and results exiting the system. However, organizations often have many controls over this function. Modification of data is considered more of a vulnerability than modification of programs since this individual is not apt to understand enough about the programs to cause significant loss of integrity. A serious danger is that data or programs will be made unavailable. A mitigating factor is that individual operators will be able to manipulate data and programs for only those application areas that they normally service.

Computer Operator

Function. Operates a computer from the computer console, monitors computer operations, alters job schedules and priorities through the console, initiates utility program execution, responds to system error conditions according to documented instructions, mounts magnetic tapes and disk packs, powers up and powers down the system, schedules machine utilization, responds to emergencies and possible security alarms.

Knowledge. Operating system functions, utility program functions, computer processing workflow, system accounting procedures, console protocol, privileged access procedures, physical access procedures, contingency planning and security procedures, and communications protocols.

Skills. Typing and console operation, computer equipment operation, reading procedural documentation, reading and interpreting console messages.

Access. Computer operations area, computer equipment area, files stored in operations area, procedural documentation, privileged access to the computer system.

Vulnerability. The enterprise is vulnerable to both physical and operational violations from this individual. A general area of vulnerability is violations involving the availability or confidentiality of data, application programs, or systems programs internal to the system in main memory or on tape or disk. Other areas include violations affecting system service such as unauthorized use of services, those involving the physical manipulation of system equipment, and those causing loss of availability or confidentiality of data stored external to the system.

Conclusions. This individual is in a key position relative to data and programs internal to the system. Although limited to console operations and programs already in the system or transferable via telecommunications, in the absence of other controls, a clever individual in this position would be likely to be able to gain access to any data file or program so as to cause its unavailability or loss of confidentiality. This individual is also in the position to modify some data.

Peripheral Equipment Operator

Function. Operates all equipment immediately peripheral to the computer system having to do with input/output and file usage including paper tape readers, MICR readers, optical readers, tape drives, disk drives, sorters, tape cleaners, printers, paper tape punches, COM devices; loads and unloads removable media including tape, tape cartridges, disk packs, printer listings; installs expendable supplies on the equipment; sorts and labels output.

Knowledge. Computer processing work flow, system accounting procedures, media library, physical access procedures.

Skills. Peripheral equipment operation, reading procedural documentation.

Access. Peripheral equipment area, job setup area, user output distribution area, input data, output results, procedural documentation, expendable supplies.

Vulnerabilities. The enterprise is vulnerable to both physical and operational violations from this individual. The principal area of vulnerability is violations of availability or confidentiality of data, application programs, and systems programs external to the system but in the general operations area. A secondary vulnerability has to do with destruction or taking of equipment or supplies.

Conclusions. Although this individual will have access to much input data and output results, the physical situation is likely to be such that copying this information for the purpose of disclosure will be difficult. Certainly it will be somewhat easier to destroy such information.

Job Setup Clerk

Function. Assembles jobs including data, programs, and job control information and physically places this material into job queues; requests data from media library; handles procedures for reruns and extraordinary user requests; may also distribute output results.

Knowledge. Computer processing workflow, system accounting procedures, media library, physical access procedures.

Skills. Reading job-related documentation, manual capabilities to handle punch cards and magnetic tapes.

Access. Job setup area, user output distribution area, input data, procedural and data base documentation, possibly also some media storage and other off-line files.

Vulnerabilities. The enterprise is vulnerable to both physical and operational violations from this individual. The principal area of vulnerability is violations of availability or confidentiality of data or application programs external to the system but in the general operations area. A secondary vulnerability is destruction or taking of media; a tertiary and remote possibility is the taking of system service.

Conclusions. Although this individual will have access to much input data and many application programs, the physical situation is likely to be such that copying this information for the purpose of disclosure will be difficult. Certainly it will be somewhat easier to destroy such information. As mentioned above, the possibility of the individual taking system service exists but is very remote because of the individual's lack of knowledge about how the system works.

Data Entry and Update Clerk

Function. Adds, changes, or deletes records in data bases by means of on-line terminal entry or manual entries on data input forms.

Knowledge. Data base concepts; data base languages; data base files, formats, and content; security access controls; terminal protocol; identification/verification procedure; to some extent, computer processing workflow.

Skills. Typing and terminal operation, reading procedural documentation.

Access. Terminal area, data source documents, terminal operation instructions, identification/verification materials, on-line files, documentation on data base structure and content, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical and operational violations by this individual. The principal area of vulnerability is violations that involve the loss of availability or confidentiality of data, application programs, or systems programs either internal or external to the system. In addition, this individual has the opportunity to modify data either internal or external to the system and to commit violations having to do with destruction and taking of terminal equipment.

Conclusions. This individual is in a key position relative to data entering the system. Unlike many positions, this individual can cause all kinds of data loss. The danger of external manipulation of data is somewhat less than that for internal since not all files would likely be updated by this clerk, especially where duties and work reviews are adequately separated.

Media Librarian

Function. Files, retrieves, and accounts for off-line storage of data and programs on tape and other removable media; provides media to production control and job setup areas; cycles backup files to remote facilities.

Knowledge. File names and labels, library and job accounting procedures, computer processing workflow, physical access procedures, archived files.

Skills. Reading procedural documentation, record keeping and filing.

Access. Tape library, current and aging program and data files, interface to off-site remote storage facilities and to production control.

Vulnerabilities. The enterprise is vulnerable to physical violations from this individual. The principal area of vulnerability is violation of availability or confidentiality of data or programs stored external to the system on removable media. A secondary area is violations involving the destruction or taking of the media.

Conclusions. Lack of knowledge as to the content of the files being handled limits the likelihood of fraud by this individual. Physical manipulation of the media with the intent to vandalize is more likely.

Systems Programmer

Function. Designs, develops, installs, documents, and maintains operating system and utility software, including programming language compilers, loaders, linkage editors, input/output routines, storage management software, program library access and maintenance routines, terminal and communication line handlers and other programs, system debugging facilities, system access controls, job scheduling routines, system accounting facilities, interrupt and trap servicing programs, sorting and mathematical utility programs, database packages, modification of programs.

Knowledge. Operating systems, programming languages, terminal and computer console protocols, identification/verification procedures, computer processing workflow, hardware system architecture, elementary mathematical functions, Boolean algebra, number systems, alphanumeric codes, application programs, system integrity and security, system planning, network planning.

Skills. Programming and documentation, computer and peripheral equipment operation, reading and analyzing memory dumps and flowcharts, general diagnostic analysis, communication linkages.

Access. System programming area, system documentation, privileged access to the computer and data communications systems.

Vulnerabilities. The enterprise is vulnerable to physical, operational and programming violations by this individual. A principal area of vulnerability is violations that cause loss of availability or confidentiality of data, application programs, or systems programs internal to the system in main memory or on tape and disk either by direct, real-time actions or by causing system programs to lose integrity. In addition, this individual can modify systems programs internal to the system and cause all types of losses involving systems programs external to the system. Another major area of vulnerability is violations that make unauthorized use or deny, delay, or prolong authorized use of system services. A secondary area is violations that involve the destruction or taking of terminal equipment.

Conclusions. This individual is in a position to attempt violations in a number of areas and the categories of safeguards mentioned above are apt to have less than total effectiveness in dealing with a clever systems programmer. Also, all safeguards implemented in software may have limited value since systems programmers are responsible for the design, implementation, and maintenance of such software and have privileged access to the system. This threat of destruction of system programs external to the system is not so serious, however, because most of them would be backed up with copies on the system.

Application Programmer

Function. Designs, develops, installs, documents, and maintains application programs and systems using a variety of programming languages.

Knowledge. Programming languages, EDP procedures and concepts, terminal protocols, identification/verification procedures, elementary mathematical functions, number systems, alphanumeric codes, business needs.

Skills. Programming and documentation, programming terminal operation, reading and analyzing memory dumps and flowcharts, general diagnostic analysis.

Access. Application programming area, application programs and their documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, and programming violations by this individual. A principal area of vulnerability is violations that involve all types of losses of application programs either internal or external to the system. The individual may also modify, destroy, or disclose the parametric data for his pro-

grams. A secondary area of vulnerability is violations that involve the unavailability of terminal equipment.

Conclusions. This individual has limited accessibility to areas and facilities that would enable attempts at violations. Essentially, the only access is to application programs and just the fraction of those the individual is involved with. Conversely, the individual's role regarding these application programs makes it very difficult to ensure that safeguards against violations will be effective.

Terminal Engineer

Function. Tests, diagnoses, repairs, replaces, assembles, and disassembles terminals, components, and other equipment.

Knowledge. Electronic, mechanical, and communication engineering; digital logic design; physical access procedures; Boolean algebra, vendor products.

Skills. Operation of computer and electronic test equipment, reading circuit schematics and diagnostic manuals.

Access. Computer and adjacent facilities, network diagram, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, and engineering violations by this individual. The principal and only area of serious vulnerability is violations that involve terminal equipment.

Conclusions. Allowing a well-trained person access to a terminal would appear to pose a multifaceted threat to system security. Vulnerability is to physical manipulation of terminal equipment and to other logical forms of unauthorized access to data.

Computer Systems Engineer

Function. Tests, diagnoses, repairs, replaces, assembles, and disassembles computer system hardware and components including computers, terminals, peripheral devices, and communication equipment.

Knowledge. Electronic, mechanical, and communication engineering, programming languages, digital logic design, terminal protocols, physical access procedures, Boolean algebra.

Skills. Operation of terminals, computer consoles, peripheral devices, communication equipment, and electronic test equipment, programming and documentation, reading and analyzing memory dumps and flowcharts, reading circuit schematics and diagnostic manuals, general diagnostic analysis.

Access. All equipment and adjacent facilities, some system programs with documentation, documentation for all equipment, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, programming, and engineering violations by this individual. The two principal areas of vulnerability are violations that involve all types of losses associated with system equipment and those that involve unauthorized use or denial, delay, or prolongation of authorized use of system service. A secondary area is violations that involve loss of intent, availability, or confidentiality of system programs internal to the system.

Conclusions. This individual poses as great a threat as anyone in the installation to physical abuse of system equipment and manipulation of system service. Although he or she might appear to have ready access to other sensitive areas as well, controls can be instituted to minimize the vulnerability in these other areas.

Communication Engineer and Technical Specialist

Function. Tests, diagnoses, repairs, replaces, assembles, disassembles, and operates data communications equipment including concentrators, multiplexors, modems, and line switching units; reconfigures communication network when necessary.

Knowledge. Electronic and communication engineering, data communication, terminal protocols, identification/verification procedures, physical access procedures, Boolean algebra.

Skills. Operation of terminals, communication equipment, and electronic test equipment, reading circuit schematics and diagnostic manuals, reading procedural documentation.

Access. Communication equipment and adjacent facilities, circuit and network diagrams, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, and engineering violations by this individual. The principal area of vulnerability is violations that involve the loss of availability or confidentiality of data internal to the system and being transmitted in the communication system. A secondary area is violations that involve the modification, destruction, or taking of terminal or communication equipment.

Conclusions. Although this individual is in a position to intercept data for later violation of confidentiality, he or she is not likely to have enough knowledge about the data files to be able to make a judicious selection of materials

to disclose. The threat from this individual is greater in the area of malicious acts that would serve to disrupt computer processing such as destruction of data files or manipulation of terminal or communication equipment.

Facilities Engineer

Function. Inspects, adjusts, diagnoses, repairs, replaces, assembles and disassembles equipment supporting computer and terminal equipment, such as power, water, light, heat, water chilling, and air conditioning equipment.

Knowledge. Electrical and mechanical engineering, physical access procedures.

Skills. Use of test equipment; reading building, circuit, and engineering schematics; reading diagnostic manuals.

Access. All building areas, building and support equipment diagrams and documentation.

Vulnerabilities. The enterprise is vulnerable to physical violations by this individual. The two principal areas of vulnerability are violations that involve denial, delay, or prolongation of authorized system service and destruction or taking of system equipment. A minor area is the loss of integrity of system support equipment.

Conclusions. This individual's authorized access to all areas facilitates malicious acts that would serve to disrupt system operation. Similarly, the person has greater opportunity than most to take system and system support equipment. Also, because of the individual's authorized access, prevention safeguards will not likely be very effective in this case.

Operations Manager

Function. Designs, develops, installs, schedules, modifies, documents, maintains, and manages the computer processing workflow system through direction given to operational subordinates; also responsible for physical security of system equipment, as well as data and programs on removable media stored in the operations area; responsible for security, quality control, and general operations.

Knowledge. Computer processing workflow system, hardware configuration architecture, operations procedures for data files, media storage, job accounting, physical access, and system integration and maintenance, operating system and utility software, database systems.

Skills. Developing and reading flowcharts, principles of operation manuals, and other procedural documentation; performing systems analysis and general diagnostic analysis; management.

Access. Computer and peripheral equipment facilities; job input/output, scheduling, and servicing areas; tape library and its media contents; system documentation and all procedural documentation; data files; application programs; and systems programs internal to the system.

Vulnerabilities. The enterprise is vulnerable to physical and operational violations by this individual. The primary areas of vulnerability are causing the loss of availability or confidentiality of data, application programs, or systems programs internal to the system, destruction or taking of system equipment and unauthorized use or denial, delay, or prolongation of authorized use of system services. In addition, this individual can destroy or disclose those data files, application programs, and system programs that are stored in the tape (or media) library, and can modify parametric data either internal or external to the system.

Conclusions. As mentioned above, this individual is in a position to attempt many categories of violations. Also, many of the safeguards against possible violations are the responsibility of the DP department of which he or she is a key member. Fortunately, many DP departments have a system control group on the same level as this individual's operations group. Almost all safeguards of the DP department that are intended to thwart serious violations by this individual are the responsibility of the system control group or the DP department top management. Note that the destruction of system programs external to the system by this individual is not so serious since most of these programs are likely to be backed up in the system.

Data Base Administrator

Function. Responsible for adding, changing, and deleting records in on-line and off-line data bases and other data resources, data integrity and security, contingency planning.

Knowledge. Data base concepts, data base languages, data base files, formats, and content, computer processing workflow, security access controls, terminal protocol, identification/verification procedure, data usage patterns, physical data structures, logical views of data elements.

Skills. Typing and terminal operation, reading procedural documentation, performing general diagnostic analysis.

Access. Terminal area, tape (or media) library in the operations area, on-line files, data source documents, documentation on data base structure and content, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical and operational violations by this individual. The first area of serious vulnerability to actions by this individual is his internal and external access to all data maintained by the

DP department; since one responsibility of this person is modifying these files, the operation is vulnerable to integrity loss of data as well as to destruction and disclosure. A secondary area of vulnerability is violations that involve destruction or taking of terminal equipment.

Conclusions. With the proper organization of the DP department, this individual will not be administering safeguards that are designed to thwart violations. The nature of this person's responsibility makes detecting the violations particularly difficult.

Programming Manager

Function. Designs, develops, installs, documents, and maintains application programs through direction given to subordinates.

Knowledge. Programming languages, EDP procedures and concepts, application subject areas, advanced programming and software engineering techniques, data base design procedure, terminal protocol, identification/verification procedures, computer processing workflow, elementary mathematical functions, number systems, alphanumeric codes.

Skills. Programming and documentation, terminal operation, reading and analyzing memory dumps and flowcharts, systems and general diagnostic analysis, management.

Access. Application programming area, application programs and their documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, and programming violations by this individual. A principal area of vulnerability is violations that involve all kinds of losses associated with application programs either internal or external to the system. The individual may also modify, destroy, or disclose parametric data for the programs he or she is responsible for. A secondary area of vulnerability is violations that involve the destruction or taking of terminal equipment.

Conclusions. This individual has limited accessibility to areas and facilities that would facilitate violations. Essentially, access is limited to the application programs generated and maintained by the group. Conversely, this person's role in the development of these application programs makes it very difficult to ensure that safeguards against actions will be effective.

Information Security Officer

Function. Plans, implements, installs, operates, maintains, and evaluates physical, operational, technical, procedural, and personnel-related safeguards and controls.

Knowledge. Security (including identification) concepts; EDP software and hardware technology; industrial security products; procedural, operational, and personnel policies and practices.

Skills. A level of electronic, mechanical, and programming skills sufficient to allow planning and implementation of suitable safeguards, reading building, circuit, and engineering schematics, reading diagnostic manuals, reading and analyzing memory dumps and flowcharts.

Access. Privileged access to all areas and all system functions.

Vulnerabilities. The enterprise is vulnerable to all manner of violations by this individual.

Conclusions. There is virtually no possibility of detecting violations perpetrated by individuals in this position. In practice, the individual will often have insufficient knowledge and skills to attempt unauthorized acts in some areas.

EDP Auditor

Function. Performs operational, software, and data file reviews to determine integrity, adequacy, performance, security, and compliance with organizational and generally accepted policies, procedures, and standards; participates in design specification of applications to assure adequacy of controls; performs data processing services for auditors, reports findings to senior management.

Knowledge. Audit techniques, controls, safeguards, system design, software organization, computer applications, facilities security.

Skills. Use of audit tools, programming and documentation, reading technical, operational, and procedural documentation, general diagnostic analysis.

Access. Privileged access to all areas and all system functions.

Vulnerabilities. All manner of violations are possible by this individual.

Conclusions. There is virtually no possibility of detecting violations perpetrated by individuals in this position. All avenues— screening by external CPA auditors, screening by examiners from regulatory agencies, and peer review of the individual's work and activities—should be used to ascertain that the candidate is competent and trustworthy.

APPENDIX E

Audit Tools and Techniques

APPENDIX E: Audit Tools and Techniques

This appendix describes 15 audit tools and techniques and identifies the EDP occupations of people whose errors or criminal acts might be detected by these tools or techniques.

Test Data Method

The test data method verifies the processing accuracy of computer application systems by executing these systems with specially prepared sets of input data that produce preestablished results. The method enables internal auditors to verify specified and limited program functions. Tests can be expanded incrementally, and special procedures are not usually required. The test data method is not an appropriate technique for verification of production data, however; no evidence is provided concerning the completeness or accuracy of production input data or master files. The test data method affects the following occupations:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Job setup clerk	Network manager
Systems programmer	Operating manager
Application programmer	Programmer manager

Base-Case System Evaluation

Base-case system evaluation (BCSE) is a technique that applies a standardized body of data (input, parameters, and output) to the testing of a computer application system. This body of data, the base case, is established by user personnel, with internal audit concurrence, as the criterion for correct functioning of the computer application system. This testing process is most widely used to validate production computer application systems. One major manufacturing company, however, used the base-case approach "to test programs during their development, to demonstrate the successful operation of the system prior to its installation, and to verify its continuing accurate operation during its life." As such, this approach represents a total commitment by corporate management and each user department to the principles and disciplines of BCSE. The BCSE affects the following occupations:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Job setup clerk	Network manager
Systems programmer	Operations manager
Applications programmer	Programming manager

Integrated Test Facility

Integrated test facility (ITF) is a technique for reviewing those functions of an automated application that are internal to the computer. Internal auditor's test data are used to compare ITF processing results to precalculated test results. The method is most frequently used to test and verify large computer application systems when it is impractical to separately cycle test data. The ITF technique is of limited value for the verification of production data or data files; very little evidence is provided on the completeness and accuracy of production input data or master-files. ITF affects the following occupations:

Communications operator	Systems engineer
Systems programmer	Programming manager
Application programmer	

Parallel Simulation

Parallel simulation is the use of one or more special computer programs to process "live" data files and simulate normal computer application processing. Whereas the test data method and the ITF process test data through live programs, the parallel simulation method processes live data through test programs. Parallel simulation programs include only the application logic, calculations, and controls that are relevant to specific audit objectives. As a result, simulation programs are usually much less complex than their application program counterparts. Large segments of major applications that consist of several computer programs can often be simulated for audit purposes with a single parallel simulation program. Parallel simulation permits the internal auditor to independently verify complex and critical application system procedures. Parallel simulation affects the following occupations:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Communications operator	Network manager
Systems programmer	Operations manager
Applications programmer	Programming manager

Transaction Selection

The transaction selection audit technique uses an independent computer program to monitor and select transactions for internal audit review. The method enables the internal auditor to examine and analyze transaction volumes and error rates and to statistically sample specified transactions.

Transaction selection audit software is totally independent of the production computer application system and is generally parameter-controlled. No alteration to the production computer application system is required. This technique is especially suitable for noncontinuous monitoring and sampling of transactions in complex computer application systems. Transaction selection affects the following occupations:

- Transaction operator
- Peripheral operator
- Data entry and update clerk
- Communications operator
- Terminal engineer
- Communication engineer
- Network manager
- Operations manager
- Data base manager
- Identification control clerk

Embedded Audit Data Collection

Embedded audit data collection uses one or more specially programmed data collection modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the computer application system at points determined to be appropriate by the internal auditor. The internal auditor also determines the criteria for selection and recording. After collection, other automated or manual methods may be used to analyze the collected data.

As distinct from other audit methods, this technique uses "in-line" code (i.e., the computer application program performs the audit data collection function at the same time it processes data for normal production purposes). This has two important consequences for the auditor: in-line code ensures the availability of a comprehensive or a very specialized sample of data (strategically placed modules have access to every data element being processed); retrofitting this technique to an existing system is more costly than implementing the audit programming during system development. Internal auditors therefore prefer to specify their requirements while the system is being designed. Embedded audit data collection affects the following occupations:

- Transaction operator
- Computer operator
- Peripheral operator
- Job setup clerk
- Data entry and update clerk
- Communications operator
- Terminal engineer
- System engineer
- Communications engineer
- Network manager
- Operations manager
- Data base manager
- Identification control clerk

Extended Records

Using a special program or programs, the extended records technique gathers together all the significant data that have affected the processing of an individual transaction. Such extended records are compiled into files that provide a conveniently accessible source for transaction data.

With this technique, the auditor no longer need review several files to determine how a specific transaction was processed. With extended records, data are consolidated from different accounting periods and different computer application systems to provide a complete transaction audit trail in one computer record. This facilitates tests of compliance to organization policies and procedures. The extended records technique affects the following occupations:

- Transaction operator
- Peripheral operator
- Data entry and update clerk
- System programmer
- Application programmer
- Terminal engineer
- Systems engineer
- Communication engineer
- Network manager
- Operations manager
- Data base manager
- Programming manager
- Identification control clerk

Generalized Audit Computer Programs

Generalized audit computer programs are the most widely used techniques for auditing computer application systems. These products permit the internal auditor to independently analyze a computer application system file. Because of their widespread use and long history, most generalized audit packages are ultrareliable, highly flexible, and extensively and accurately documented. Generalized audit programs can be used to foot, cross-foot, balance, stratify, select a statistical sample, select transactions, total, compare, and perform calculations on diverse data elements contained within various data files. Generally, this audit method is used to test computer file data; little facility is present to test system logic, other than implicitly by the results that appear in the data files. No explicit compliance testing facility is contained in these programs. Historically, generalized audit programs are operated only in the batch mode. With the rapid expansion of on-line computer application systems, on-line generalized audit programs have become available. Use of generalized audit programs affect the following occupations:

Transaction operator
Computer operator
Peripheral operator
Job setup clerk
Data entry and update clerk
Communications operator
Media librarian
Systems programmer
Application programmer
Terminal engineer
System engineer
Communication engineer
Network manager
Operations manager
Data base manager
Programming manager
Identification control clerk

Snapshot

Both internal auditors and data processing personnel periodically encounter difficulty in reconstructing the computer decision-making process. The cause is a failure to keep together all the data elements in that process. Snapshot is a technique that, in effect, takes a picture of the parts of computer memory that contain the data elements in a computerized decision-making process at the time the decision is made. The results of the snapshot are printed in report format for reconstructing the decision-making process.

The technique requires the logic to be preprogrammed in the system. A mechanism, usually a special code in the transaction record, is added to trigger the printing of the data in question for analysis.

The snapshot audit technique helps internal auditors answer questions on why computer application systems produce questionable results. It provides information to explain why a particular decision was developed by the computer. Snapshot audit used in conjunction with other audit techniques (e.g., integrated test facility or tracing) determines what results would occur if a certain type of input entered the data processing system. The snapshot audit technique also can help systems and programming personnel in debugging the application systems. The snapshot audit affects the following occupations:

System programmer
Application programmer
Terminal engineer
Systems engineer
Communication engineer
Network manager
Data base manager
Programming manager

Tracing

A traditional audit technique in a manual environment is to follow the path of a transaction during processing. For example, an auditor picks up an order as it is received into an organization and follows the flow from work station to work station. The internal auditor asks the clerk involved what actions were taken at that particular step in the processing cycle. Understanding the policies and procedures of the organization, the internal auditor can judge whether they are being adequately followed.

After walking through the processing cycle, the internal auditor has a good appreciation of how work flows through the organization. In a data processing environment, the auditor cannot follow the path of a transaction through its processing cycle solely by following the paperwork flow. Many of the functions performed by clerks and the movement of hardcopy documents are replaced by electronic processing of data.

The tracing audit technique enables the internal auditor to perform an electronic walk-through of a data processing application system. Tracing shows what instructions have been executed in a computer program and in which sequence they have been executed. Because the instructions in a computer program represent the steps in processing, the processes that have been executed can be determined from the results of the tracing audit technique. Once an internal auditor knows what instructions in a program have been executed, the auditor can determine if the processing conformed to organization procedures and policies. The tracing technique affects the following occupations:

Systems programmer
Application programmer
Terminal engineer
Systems engineer
Communication engineer
Network manager
Programming manager

Mapping

Mapping is a technique for assessing the extent of system testing and for identifying specific program logic that has not been tested. Mapping is performed by a program measurement tool that analyzes a computer program during execution to indicate whether program statements have been executed. This measurement tool can also determine the amount of CPU time consumed by each program segment.

The original intent of the mapping concept was to help computer programmers ensure the quality of their programs. However, auditors can use these same measurement tools to look for unexecuted code. This analysis can provide the auditor with insight into the efficiency of program operation and can reveal unauthorized program segments included for execution for unauthorized purposes. The mapping method affects the following occupations:

System programmer
Application programmer
Program manager

Control Flowcharting

In a complex business environment, thoroughly understanding an organization's total system of control is difficult. A graphic technique, or flowchart, simplifies the interrelationships of controls and assists analysts or auditors in evaluating the adequacy of those controls. Flowcharts can also indicate whether controls are operating as originally intended. The control flowchart technique provides the documentation necessary to explain the system of control. Control flowcharting affects the following occupations:

- Communications operator
- System programmer
- Application programmer
- Network manager
- Operations manager
- Data base manager
- Programming manager

Job Accounting Data Analysis

Job accounting facilities are available through most computer vendors as an adjunct to their operating systems. The job accounting facility is a feature of the computer operating system software that provides the means for gathering and recording information to be used for billing customers or evaluating systems usage. Examples of information collected by a job accounting facility are job start and completion times, usage of data sets, and usage of hardware facilities. These job accounting systems were designed by the vendors to serve the operating needs of the data processing department. However, much of the information provided by these facilities is of interest to internal auditors.

Two types of job accounting data, the accounting records and the data set activity records, are of interest to the internal auditor. Accounting records consist of records that show which user used which programs, how often, and for how long. They include an identification of the user, the hardware features required by the job, the time it took to perform the job, and how the job was completed. Data set activity records provide information about which data files were used during processing and who requested the use of the data sets. Among the information contained in these records are the data set name, record length, serial number of the volumes, and the user of the data set.

The internal auditor can use data from the accounting records to verify charges for use of the computer resources. They also enable the auditor to verify that only authorized individuals use the computer. Data set activity records enable the auditor to verify that data are being used by authorized individuals. The job accounting data analysis affects the following occupations:

- Transaction operator
- Computer operator
- Application programmer
- Network manager
- Peripheral operator
- Job setup clerk
- Communications operator
- Media librarian
- Operations manager
- Data base manager
- Programming manager
- Identification control clerk

System Acceptance and Control Group

When the EDP auditor decides to monitor and review the computer application development process, the auditor must determine how to best perform the review. Although the substance of the review is unchanged, the EDP auditor may choose to perform the review personally or to rely on the efforts of another group. To perform the review personally is the choice made by many EDP auditors, even though substantial effort and training may be required to do an effective job. Much of the training required has to do with data processing rather than with EDP auditing. This, among other factors, caused the auditors at several large companies to choose another approach. These companies establish a Systems Acceptance and Control (SAC) Group in the data processing department to perform systematic reviews of computer application system developments and to create and maintain effective computer application system standards, particularly in the area of auditability. The SAC approach affects the following occupations:

- System programmer
- Application programmer
- Terminal engineer
- System engineer
- Communication engineer
- Programming manager

Code Comparison

Code comparison entails comparison of two copies, made at different times, of the program coding for a particular application. The objective of this technique is to verify that program change and maintenance procedures and program library procedures are being followed correctly. The auditor uses the output of the comparison to identify changes that have occurred between the making of the two copies. The auditor then locates and analyzes the documentation that was prepared to authorize and execute the changes. This technique supports compliance testing rather than substantive testing. Code comparison is especially useful for auditing programs that perform critical business functions and are subject to continuing change. The code comparison technique affects the following occupations:

- Computer operator
- Job setup clerk
- System programmer
- Application programmer
- Terminal engineer
- System engineer
- Communication engineer
- Operations manager
- Programming manager

APPENDIX F

Computer Intrusion Contingency and Recovery Guidelines

APPENDIX F: Computer Intrusion Contigency and Recovery Guidelines

This section lists recommendations for mitigating, investigating, and recovering from the contingency of telephone and computer terminal intrusion into a mainframe computer system and network. These recommendations are presented from the victim's perspective and indicate advice that criminal justice agencies should give to victims. The recommendations also provide insights for investigators about the victims' expectations of assistance and the methods that investigators can use to integrate their expertise and objectives with those of the victims.

1. Monitor Published Material for Information on Intruders

The various clearinghouses of information on hackers should be monitored, especially when computer intrusion is suspected. Such resources include John Maxfield's Boardscan Company, the SRI Risks Forum from SRI International, 2600 Newsletter (an underground newsletter that might be illegal to distribute in some states), Dockmaster from the U.S. NSA, and numerous security journals. Intrusion reports in technical journals provide useful background information. Valuable information also can be obtained from the recent experience of other victims and news media accounts of current incidents.

2. Decide on When and Under What Circumstances to Confront Suspected Intruders

The most critical part of addressing the intrusion contingency is the decision on whether to reveal to or keep secret from the intruder that the intrusion has been detected. Informing intruders or leaving obvious evidence of discovery may stop them, or it may spur intruders to do more mischief or boast of their success to others, who might likewise intrude. In any case, this eventuality should be weighed before a planned confrontation. The intruder should be confronted only after the other steps identified in this section have been taken or considered. Only sworn criminal justice officers authorized to make arrests should confront the suspect. The time, place, and circumstances should be prearranged with the authorities to minimize the potential negative effects on the victimized company. For example, establishing legal constraints on suspects' subsequent actions may be necessary to stop further intrusions or dissemination of information about the incident.

3. Hold All Information about Intrusion Experience on a Confidential and Need-to-Know Basis

Only those personnel who have a need to know should be informed of the intrusion and then only with essential information. For example, potential victims of similar attacks, as well as computer users, should be warned that the computer or network may no longer be under the company's exclusive control. Management and data processing personnel who may be able to provide direct assistance should be informed. Others who should be informed are members of the corporate security department, public affairs, human resources, auditors, insurance risk managers, top management, and legal counsel.

Those directly involved should meet frequently to keep up to date on current developments and to counter harmful rumors that may circulate. All information about the incident should be kept out of electronic mail and BBS types of communications where it could be obtained by the intruder. Publicly reporting selected information about the intrusion may be necessary if news media sources already know about it. Potential embarrassment may be reduced or reversed by publishing selected information as a public service to warn customers or other potential victims of similar types of incidents, especially if positive information about how effectively the incident is being handled can be produced. Public news releases should be carefully prepared in coordination with a public relations company or the internal public affairs staff as necessary. All news media should be scanned for information on the event; a clipping file of the news stories is valuable.

4. Check on Legal Liability

Legal counsel should be contacted to determine the liability of the victim's organization for possible third-party damage that could be attributed to its actions or inactions. If other computer centers or systems suffer losses because of an initial intrusion into the computer and subsequent access through data communications to their computers, liability may become an important issue.

5. Report the Incident to Appropriate Criminal Justice Agencies

The organization has a social and moral responsibility to report any suspected crimes to the authorities. The report should be made by an official spokesperson who has received top management approval and has been briefed by legal counsel, public affairs, insurance risk management, and corporate security. The conditions under which the decision to prosecute a suspect will be made should be specified. Applicable statutes should also be studied thoroughly; in particular, the two federal computer fraud and communications crime laws may apply as well as the state statutes on computer crime within the states where intrusion activity has occurred.

The applicable legal jurisdictions should be identified and the incident reported to all appropriate agencies, although some law enforcement agencies may have adversarial relationships. The agencies should decide which one is to handle the case, unless special circumstances dictate otherwise. The corporate security staff is usually aware of these relationships and can provide guidance. In the United States, the FBI, Postal Authorities, and Secret Service usually have jurisdiction in federal cases; the city police and county sheriff usually have jurisdiction at the state level. In other countries, jurisdictions may vary, and competent legal counsel should be obtained to assist in the choice.

6. Keep a Detailed Master Logbook of All Events

One person should be responsible for documenting all events and evidence of the intrusion. In addition, a list of all participants and stakeholders and their roles and information supplied to them should be maintained. Managers should frequently review the logbook to ensure it is complete. Information potentially harmful to the organization, staff, or other victims in terms of litigation or insurance claims should be kept in a separate log under the legal counsel's control. The logbook should be organized so that intrusion activity on different dates can be compared. A histogram of active times of intrusion may be useful to analyze times of day and periods of use during the intrusion.

The losses should be quantified as much as possible, particularly in terms of the opinions of users and victims who have lost data or services and the amount and cost of staff time taken in dealing with the intrusion. These figures should include the time needed by legal counsel, human resources staff, public affairs, personnel, and others.

7. Protect All Evidence from Tampering and Disclosure

All materials associated with the intrusion and investigation, including pertinent computer logs, tapes and disks, and particularly the logbooks, should be locked up. All the people involved in the mitigation and investigation of the intrusion must secure their materials. The intruder should be assumed to have access to all operational information about the compromised computers and networks. Information about the intrusion or investigation should not be entered into any computer to which the intruder may have access. All communications should be carefully used to avoid alerting the intruder. In fact, messages that the intruder may see should be produced to give the intruder as much comfort and feeling of safety as possible.

8. Trace the Intruder's Telephone Number

The intruder should be baited with attractive user accounts and data files that are heavily instrumented to monitor their access and usage. One objective is to keep the intruder active in the computer system or in use of telecommunications equipment long enough for the authorities to trace the sources of calls using pen registers, dialed number recorders (DNR), copies of telephone services billing, and DNFS equipment to record the numbers called. A detailed record of all people who access the baited accounts and files should be kept. Postal addresses should be included to lure the intruder into sending paper mail that can be collected as evidence. Paper is far superior to electronic media for evidence.

9. Install and Use Monitoring Equipment

Serial line analyzers, recorders, and printers should be installed on all incoming ports and then monitored and controlled through microcomputers. All keystrokes, keywords, and passwords used against identifiable targets should be captured. Printing should be done in real time and recorded on a disk in another computer.

Monitoring should be entirely external. Monitoring through the operating system or modifying the operating system (which is often the subject of attack) would alert the suspect, and a sufficiently skilled intruder could overcome or deceive the system.

Computer activity should be monitored for possible attacks on any other computers in the network. Audible alarms should be set to indicate when the intruder is on line. A modem can be used to call the computer operator on a pocket pager. The high volume of monitoring data can be reduced by covering only the intruder's patterned practices and stolen accounts.

The intruder's usage should be disabled only when real damage is imminent. This takes careful monitoring and anticipation of the intruder's acts. The intruder can be disabled by imposing line noise in ways that appear natural.

All internal and external clocks must be synchronized so that the timing in computer audit logs can be matched.

Clocks should be synchronized in other computers in a network that may also be subject to attack. System accounting records should be matched with external monitoring records, since the business records exception rule for hearsay evidence of the attack will probably require records gathered in the normal course of system use. The results from the additionally installed external monitoring equipment may not be accepted as evidence because of the special nature of the monitoring.

10. Trace Communications Networks to the Source of the Intrusion

Tracing telephone calls requires a court order as well as the cooperation of the telephone company and various network organizations. AT&T has several call-time specialists handling all such requests. Court orders must be obtained through criminal justice agencies—emphasizing the critical need to report such incidents to the authorities.

Criminal justice agencies and various communications companies may be uncooperative because of the significant effort required. Presenting a convincing description of a significant case to the authorities and communications companies may assist in gaining their cooperation. In addition, appeals to legislators or pressure from top management may also help.

To be sufficient for prosecution, physical observation or physical evidence obtained at the intruder's work station must be synchronized with the time when evidence of computer access through the communication line is identified.

Telephone billings provide useful evidence as well. In packet-switched communication networks, the timing of a round-trip packet acknowledgment over each network link can be measured to empirically produce delay times to different potential intruder sites. Estimated average delay times as functions of distance can then be calculated to aid in focusing on specific geographic locations of possible intruder sites.

11. Restore the Integrity of Damaged Systems

Systems can be restored by rebuilding operating systems from vendor-supplied copies and rebuilding applications from source code. System utilities should be compared with master copies to be assured of their integrity. All passwords must be changed, and users must be recertified. These tasks could be a major operation in a large system with many users. Expired accounts should be deleted, erased files purged, shared accounts eliminated, and users educated on secure system use. Finally, the vulnerabilities of the system should be analyzed and measures adopted to bring the system up to a prudent baseline level of security.

12. Gain Cooperation and Cut Bureaucratic Red Tape

In mitigation and recovery, many unusual actions will have to be taken and unusual assistance obtained from many sources. A good case must be presented and diplomacy used to gain the cooperation of the key people required. Establishing efficient, quick means of obtaining equipment and assistance may require the elimination or reduction of bureaucratic procedures.

13. Employ Ethical Practices

People's rights should not be violated during the surveillance and monitoring activities. Informed consent of those people and organizations called to assist or cooperate is an important ethical consideration.

14. Obtain a Sufficient Budget

The contingency and recovery effort should be well financed and sufficient staff time made available. Expensive outside services and additional equipment may be required. Development of a budget for contingency plans is useful.

15. Publicly Report the Experience to the Profession

After the case is closed and litigation is complete, the incident should be reported and published widely, but at a prudent level of detail (to preserve and assure the confidentiality of security controls and practices). Such reporting can help others with similar problems.

An orderly way of publicly presenting the case is to hold a press conference through the public affairs department. The presentation should describe the victimized organization in the best possible light, without directly revealing the weaknesses and embarrassing the organization unnecessarily.

APPENDIX G

Advance Preparations and the Actual Search

APPENDIX G*: Advance Preparations and the Actual Search

I. Investigative Techniques

A. Record checks:

1. Attempt to learn as much information about the personal computer owner as possible, such as:

a. Number of occupants in the private residence and their relationships.

b. Employment and educational background to determine which resident is likely to be a computer user.

2. Review telephone records:

a. Often computer sites have multiple lines (e.g., one for the bulletin board operation, one for outbound data traffic, one for voice communications).

b. Long-distance dialing company records are valuable for determining long-distance access code abuse.

B. Informants:

1. Use the informant to acquire evidence before a search warrant is prepared.

2. Use the informant to better understand the computer habits, skills, and knowledge of the suspect; identify:

a. Time of operation of target computer.

b. Nature and frequency of the illegal activity.

c. Type of computer system used by the suspect.

d. Identity of criminal associates or conspirators.

e. Occupations and employers of suspects and other people on the premises.

C. Surveillance of computer facilities

D. Pen register or dialed-number recorder (DNR):

1. If telephone access codes are being abused, use pen registers or DNRs to gather documentation. Frequently, a prosecutable case is made through the application of this technique alone.

2. Use this technique to obtain additional criminal intelligence on additional suspects, target computer systems, and the extent of computer use.

E. Undercover computer communications with targeted system and suspects:

1. Consider setting up an electronic bulletin board operation or attractive host computer system that the suspect can access or attack. However, this method is costly and requires a substantial commitment of personnel to monitor the operation.

2. If the suspect maintains his own electronic bulletin board, consider the feasibility of using a computer to gain access to his system within the provisions of the Electronic Communications Privacy Act of 1986 (PL 99-508). Frequently, suspects allow others to access their systems, which may contain unauthorized credit card information, hacking data, and access code files. Consider consensual use of an informant's access to the suspect's computer system.

F. Monitoring of computer transmissions

G. False computer data base entries as an investigative tool:

1. Credit bureaus and credit card issuers frequently allow false information to be "planted" in their data bases for law enforcement use.

2. If the suspect uses this information, the investigator can collect evidence through computer audit trails.

*Source: Stephen Purdy, "Advance Preparations and the Actual Search," Secret Service, report prepared for the Federal Computer Crime Investigation Committee (1988).

II. Supplies Needed to Execute a Search of a Personal Computer Site

A. Diskettes or portable data storage units:

1. Be prepared to copy files for temporary storage onto 5-1/4- inch, 3-1/2-inch, or 8-inch diskettes. Up to 100 diskettes may be necessary for large storage devices of 50 megabytes or more. Diskettes should be preformatted to avoid contamination when the suspect's computer is used.

2. Have a sufficient supply of tape cartridges. Some computer systems include cartridge-tape decks used for mass storage backup of hard disk information or for individual program storage.

3. Have plenty of evidence tape, adhesive labels, or some other means of write-protecting the disks.

4. Have a set of utility computer programs for target computers to retrieve data files.

B. Adhesive colored labels for use in identifying and cataloging evidence (usually supplied with new diskettes):

1. Place labels on diskette copies specifying the access commands, the operating system name in which the diskette is formatted, perhaps the program application used to create the data, and the case or file number of the investigation.

2. These labels are distinctly different from evidence labels discussed in the evidence inventory section. These labels are placed on each diskette indicating the type of information it contains.

C. Computer system manuals for the target system and programming languages

D. "Sterile" operating system diskettes. Hackers have modified operating system diskettes so that when the system is booted by other than the system's owner, a hidden subroutine is activated that destroys information on the diskettes.

E. A technically competent person to answer questions

F. Extra form-feed paper

G. The location of a computer supply store that handles the target system

H. Pen registers to download auto-dialer codes and numbers, and telephone numbers and access codes stored in the resident memory of a programmable telephone.

III. Initial Approach to the Target System

A. Do not allow anyone to disconnect the power, touch the keyboard, or in other ways alter the computer's current state.

B. Video tape the site to document the system configuration, wiring scheme, and the condition of the site on arrival. Take still photographs of recording equipment serial numbers, model numbers, and wiring schemes.

C. Begin a systematic evaluation of the computer site:

1. For an electronic bulletin board operation, observe the monitor to determine whether any incriminating information is being transmitted or reviewed by the caller.

a. If so, let the system run and try to determine the identity of those accessing the system.

b. If not (or the electronic bulletin board is not operating), disconnect the modem only.

2. Locate printouts and miscellaneous papers containing incriminating information and secure them.

D. Following proper evidence-handling procedures, secure above items in transport cartons obtained prior to the search.

IV. Auto-Dialer (Speed Dialer or Programmable Telephone)

A. Do not disconnect the telephone or auto-dialer from its power source.

B. Connect a DNR to the telephone or auto-dialer.

C. Place outgoing telephone calls through each auto-dialer or telephone number storage port and obtain a printed record of the stored telephone number or telephone access code in resident memory.

D. Upon successful completion of the previous step, disconnect the auto-dialer or telephone containing illegal access codes and pack for transport to the evidence storage site.

V. Computer Dismantling Considerations

A. Locate peripheral equipment and document the system configuration and wiring scheme.

B. Determine if a hard disk drive is present. If so:

1. Obtain a printout of the directories on site.

2. Review files and locate those containing potentially incriminating information.

3. Copy potentially incriminating files to diskettes.

4. Have a suitable utility program available to examine the hard disk for erased files (e.g., on IBM compatibles, Norton Utilities is useful for this examination).

5. Determine if erased files (directory names removed but contents still available) can be recovered (e.g., on IBM compatibles, Mace and Norton Utilities may be helpful).

6. Review erased files to locate potential incriminating information.

7. Copy incriminating information to diskettes.

8. When initial examination of the hard disk has been completed, "park" the drive heads following procedures that are found in the operator's manual of some systems.

9. If the hard disk drive is a peripheral device, disconnect it and pack it in a suitable container for transport to the storage site.

C. If no hard disk is present, determine if any review of diskettes is desired on site.

1. If the suspect is cooperative and identifies diskettes containing incriminating information, write-protect them, then review them on site, and print one or two of the incriminating files. At this point, print only enough to establish the basis for the violation. If several diskettes are to be examined, label them appropriately.

2. If the suspect is not cooperative, attempt to identify diskettes that may contain incriminating information by examining the suspect's diskette labels. If the questionable diskettes are located, write-protect them and print the directory of each diskette, and the contents of a questionable file. Again, if a number of diskettes are to be examined, label them.

3. Show the printout to the suspect, after he has been properly advised of his rights, for possible use in obtaining a confession.

4. If no further review of the diskettes is necessary on site assemble and secure computer programs and documentation (much of it may be pirated) for inventory and transport to a storage site.

D. Label the cables connecting various devices to aid in the reassembly of the system at a later time.

E. Photograph the labeled equipment and cables.

F. Disassemble, tag, and inventory the equipment.

G. Carefully pack seized devices in suitable containers for transport.

VI. Reassembling System at a Remote Location

A. Write-protect all diskettes prior to review, which preserves the integrity of the evidence examination process and prevents erasing or accidental damage to information on the seized diskettes during the review process.

B. Review all seized diskettes.

1. Create a diskette log containing the following headings: "Diskette Number," "Contents," and "Disposition."

2. Using colored adhesive labels, label each diskette with a letter of the alphabet, followed by a numeral sequentially assigned to each diskette reviewed (e.g., a-1, a-2, a-3). The letter could correspond to the room where the diskette was located, or it may correspond to one of many suspects in a case, for example.

3. Review each diskette and enter its assigned number on the diskette log.

4. Under the "Contents" column of the log, briefly describe the diskette contents (e.g., games, credit card information, access code files).

5. Print a directory of the diskette and label the printout with an adhesive label bearing the same alphanumeric designation as the diskette.

6. Determine from the directory which files listed are to be reviewed.

7. Review questionable files for incriminating information or copyright violations.

8. If incriminating information is located, print the file contents and label the printout with an adhesive label bearing the same alphanumeric designation as the diskette and the directory printout.

9. Copy the incriminating files onto a formatted blank diskette established by the reviewing person specifically for that purpose. Label it appropriately as a copy for backup purposes.

10. Enter in the "Disposition" column of the diskette log the action taken with respect to the diskette (e.g., directory printed, files printed, incriminating information obtained, file copied).

11. Do not be in a hurry. Although extremely time-consuming and tedious, this process is essential for preserving evidence and locating it easily during a court case.

C. Review printouts seized on site and those printed from review of computerized information to determine the appropriate investigative follow-up.

D. Store original diskettes in a safe location, free from magnetic fields, excessive humidity, or severe temperatures.

E. If the suspect has placed the information on the diskette using some type of commercial program package (e.g., D-base III, Lotus), copy the target or incriminating file onto a separate diskette. Then, and only then, should any attempt be made to manipulate the information in the file to a readable or usable format. Even then, the copy of the file should be used and not the original data.

F. Some of the suspect's critical files may be encrypted, which would be shown as strings of meaningless characters. If so, attempt to locate the encryption program or security plug-in circuit board and description manuals. Attempting to break the code without the key will be fruitless unless the crypto algorithm is extremely simple. If the most well-known crypto algorithm DES (Digital Encryption Standard) was used and a clear text and matching encrypted text is available where the secret key was used, a competent cryptoanalyst could discover the key using several hours of a Cray 2 computer (the fastest available) but at great expense.

G. File subdirectories and files may be stored in a "hidden" status or "erased" but still present on the disk. Use commercial utility programs that can search for and obtain files of this nature.

APPENDIX H

Time-Sharing Usage Examples

APPENDIX H: Time-Sharing Usage Examples

Three examples of the use of nationally known time-sharing services are provided below to show the range of time-sharing features and methods in use.

Example 1

Table H-1 illustrates an actual time-sharing terminal output listing produced during a session using a time-sharing service. It shows the typical user interaction for this type of computer use. A line-by-line description of the exhibit follows.

The user produces lower-case type at a typewriter-like computer terminal; the computer system produces upper-case type in response to what the terminal user types, according to the computer program being used at the time. Numbers in parentheses reference lines in the table.

Equipment and System Identification (01-04)

In this sequence, the terminal user interacts with the computer's communication system and identifies the computer equipment and the operating system he wants to use.

(01) The user types the code "ba" in initializing his run, to indicate that he wishes to use the vendor's production computer and text editing system. He would have typed another 2-digit code if he wished to use different computer equipment and operating system packages available to users. The computer responds to the user's input with a protocol message that serves to identify the communication line desired.

(02) The user once again types "ba" to select the equipment and operating system he wants to use.

(03) The computer responds that the desired system is operating and is ready for the next steps in the log-on process.

(04) The computer then requests the 2-digit code that corresponds to the user's terminal type. This information is necessary so a transactional table may be used that allows different types of terminals to communicate with the same computer system. The terminal user types "aj," which is the manufacturer code for the manufacturer of his computer terminal. Use of an incorrect code will cause communication with the computer system to be garbled and unintelligible.

Table H-1

TIME SHARING LISTING: EXAMPLE 1

LINE REFERENCE	TERMINAL LISTING	
(01)	baIBUALI SYSTEM ID	EQUIPMENT & SYSTEM IDENTIFICATION
(02)	ba	
(03)	READY	
(04)	MODEL? aj	
(05)	OSI/SUPERWYLBUR: LINE 39 05/23/79 12:25:24 P.M.	LOG-ON AUTHORIZATION
(06)	LIST FROM &PUBLIC.TRAINING FOR JUNE, 1979 TRAINING SCHEDULE	
(07)	TERMINAL? t00	
(08)	ACCOUNT?	
(09)	USER?	
(10)	KEYWORD?	
(11)	ILLEGAL KEYWORD	
(12)	ACCOUNT?	
(13)	USER?	
(14)	KEYWORD?	
(15)	INITIALIZING FROM LAST SESSION	RETRIEVAL FROM FILE
(16)	? clr text	
(17)	? use from samplefile on sri001	
(18)	"SAMPLEFILE" NOT FOUND ON SRI001	
(19)	? use from &sampl***	
(20)	? use from &css.samplefile on sri001	
(21)	? list	

Table H-1 (Concluded)

LINE REFERENCE	TERMINAL LISTING
(22)	1. THIS IS A SAMPLE FILE. IT MIGHT CONTAIN SENSITIVE INFORMATION
	2. OR CONTAIN INSTRUCTIONS FOR THE COMPUTER TO PERFORM SOME
	3. RESTRICTED TASKS. IT IS PROTECTED BY SEVERAL CODES. TO READ
	4. THIS FILE YOU MUST KNOW THE ACCOUNT NUMBER, THE USER INITIALS,
	5. AND THE FILE NAME. TO WRITE ON TOP OF THE FILE YOU MUST
	6. ALSO KNOW THE THE KEYWORD ASSOCIATED WITH IT. THIS FILE
	7. COULD ALSO HAVE BEEN ENCODED IF THE CREATOR OF THIS FILE
	8. HAD SO WISHED. THEN THE READER WOULD HAVE BEEN REQUIRED
	9. TO KNOW A CODE WORD ALSO.
(23)	? insert 10,11,12
(24)	10. ? THIS LOCAL ***
	10. ? I A***
(25)	10. ? i am changing my personal copy of the file. to change the
	11. ? copy of the file used by others i must successfully "resave"
	12. ? the file.
(26)	? list
(27)	1. THIS IS A SAMPLE FILE. IT MIGHT CONTAIN SENSITIVE INFORMATION
	2. OR CONTAIN INSTRUCTIONS FOR THE COMPUTER TO PERFORM SOME
	3. RESTRICTED TASKS. IT IS PROTECTED BY SEVERAL CODES. TO READ
	4. THIS FILE YOU MUST KNOW THE ACCOUNT NUMBER, THE USER INITIALS,
	5. AND THE FILE NAME. TO WRITE ON TOP OF THE FILE YOU MUST
	6. ALSO KNOW THE THE KEYWORD ASSOCIATED WITH IT. THIS FILE
	7. COULD ALSO HAVE BEEN ENCODED IF THE CREATOR OF THIS FILE
	8. HAD SO WISHED. THEN THE READER WOULD HAVE BEEN REQUIRED
	9. TO KNOW A CODE WORD ALSO.
(28)	10. I AM CHANGING MY PERSONAL COPY OF THE FILE. TO CHANGE THE
	11. COPY OF THE FILE USED BY OTHERS I MUST SUCCESSFULLY "RESAVE"
	12. THE FILE
	DATA SECURITY
(29)	? resave
(30)	KEYWORD FOR 1896-CSS?
(31)	INCORRECT KEYWORD
(32)	REQUEST NOT EXECUTED
	RETRIEVAL FROM FILE
(33)	? use from &css.samplefile on sri001
(34)	IF IT'S OK TO CLEAR "&CSS.SAMPLEFILE", REPLY "YES"
(35)	CLEAR? yes
(36)	? list
(37)	1. THIS IS A SAMPLE FILE. IT MIGHT CONTAIN SENSITIVE INFORMATION
	2. OR CONTAIN INSTRUCTIONS FOR THE COMPUTER TO PERFORM SOME
	3. RESTRICTED TASKS. IT IS PROTECTED BY SEVERAL CODES. TO READ
	4. THIS FILE YOU MUST KNOW THE ACCOUNT NUMBER, THE USER INITIALS,
	5. AND THE FILE NAME. TO WRITE ON TOP OF THE FILE YOU MUST
	6. ALSO KNOW THE THE KEYWORD ASSOCIATED WITH IT. THIS FILE
	7. COULD ALSO HAVE BEEN ENCODED IF THE CREATOR OF THIS FILE
	8. HAD SO WISHED. THEN THE READER WOULD HAVE BEEN REQUIRED
	9. TO KNOW A CODE WORD ALSO.
	LOG-OFF
(38)	? log-off clean
(39)	05/23/79 Wednesday 12:31:09 p.m.
(40)	$0.31 CHARGE
(41)	END OF SESSION

Log-On Authorization (05-14)

In this sequence, the terminal user interacts with the operating system he specified and identifies himself as an authorized user to gain access to records stored within the computer and to use computer resources.

(05) The software package, SUPERWYLBUR, selected by the user in 02, identifies itself. "Line 39" is identified as the specific communication line that connects the user and computer; this line will serve as a reference for the computer operator should the operator need to directly communicate with the terminal user. The date and time of contact with SUPERWYLBUR also are listed.

(06) The computer operator initialized this systems message earlier; it automatically greets users to notify them of upcoming systems changes.

(07) SUPERWYLBUR requests a three-character computer terminal identification code from the user. The terminal ID code is used for billing and could be used to track activity at a specific terminal. The security potential of the terminal ID code is not utilized; the validity of the codes entered is not checked.

(08, 09, 10) The computer prompts—"ACCOUNTS?", "USER?", and "KEYWORD?"—are the primary security checks in the SUPERWYLBUR system. To gain access to certain records in the system or to use computer resources, the terminal user must type in a valid one- to four-digit account number, a valid three-digit user code, and a valid three-digit keyword. For each valid account number, the account holder establishes a limited number of user codes and divulges them to the vendor for data processing. The account holder gives each authorized user a user code. The terminal user then sets up a secret keyword on his terminal. If an unauthorized user discovers the account number and user codes, which often are not rigorously guarded, he still cannot access the system unless he can obtain the user's unique keyword, which corresponds to the account number and user code he has discovered. A series of Ms and Xs are typed one on top of the other; the terminal user types his codes on top of these "underscored" letters, which makes the codes unintelligible to the eye.

(11) The keyword typed by the user in (10) was invalid; it did not match the keyword established by the user of the account. The computer indicates this to the terminal user.

(12) After the input of an invalid keyword, the computer repeats the three security prompts by first requesting the account number code. The user responds by typing the code over the underscored characters.

(13) The account number code typed by the terminal user was valid; it matched an account number in the computer file. The computer next prompts the user for his user code, which the user types over the underscored characters.

(14) The user code typed by the user was valid; it corresponded to the account number code previously typed. The computer then prompts the user for his keyword, which he types in.

Retrieval from File (15-28)

The terminal user has just effected an authorized log-on. In this series of interactions, the user copies a file from the computer disk to a section of main memory in the CPU and performs list and add operations to the file data.

(15) After the successful log-on, the computer notifies the user that he left a file intact within the default working file of the CPU during his last session. The computer is ready to perform operations on this file as per the user's instructions.

(16) The question mark indicates the computer is waiting for a command from the user. The user gives the command to clear the "old" text from the default file.

(17) A question mark indicates that the user's request in (16) was completed, and the computer awaits another command. The user asks the computer to bring in the data set called "samplefile," which may be found on the memory disk, volume serial number SRI 001.

(18) The computer tells the terminal user that a data set called samplefile, on disk SRI 001 available to his user code and account number could not be found.

(19) Prompted by the computer for another command, the user begins to request another dataset, but makes a typing error.

(20) The computer recognizes that a mistake has been made and prompts the user for another command. The user requests the same file, samplefile, in a manner that allows him authorized access to this protected file. The originator of samplefile had declared that samplefile would only be observable to other users who knew his user code, ostensibly a small group of coworkers. Hence, the file named "samplefile" was created as a file type that requires a code—in this case, the user ID code as a prefix to the file name. The terminal user requests "samplefile" and correctly includes the user code prefix in his command.

(21) The question mark acknowledges that samplefile has been found, a copy has been transferred to the main memory, and samplefile is ready for use. The user commands the computer to list the entire file.

(22) The computer lists samplefile as commanded.

(23) Prompted by the computer for another command, the terminal user directs the computer to add three lines,

lines 10, 11, and 12 to the file. This addition will affect the file only in the main memory, not the file on disk.

(24) The question mark and "10" means the computer acknowledges the command and requests the test for line 10. The user begins typing the text to line 10, but makes a mistake and indicates this by typing three asterisks.

(25) The terminal user types the test for lines 10, 11, and 12.

(26) The question mark produced by the computer indicates that the text to lines 10, 11, and 12 have been added to the copy of samplefile within the main memory. The user commands the computer to list this copy so he can visually verify the addition.

(27) Lines 1-10 are the original samplefile.

(28) Lines 10-12 are the added lines. The user can see that the main memory copy of samplefile includes his addition.

Data Security (29-32)

In this interaction sequence, the user attempts to modify the original copy of samplefile on the disk. To do so, he must comply with the data security checks put on samplefile by its originator.

(29) The user commands the computer to rewrite the altered 12-line file onto the original file copy.

(30) Because it is not his own data set he is altering, the terminal user is prompted to give the keyword that corresponds to the user code of the person who originated samplefile. The computer refers to samplefile by the account number "1896" and the user code, "CSS." In doing so, the account number is openly revealed for the first time, and the user code is openly revealed for the second time [see (20)]. Hence, a perpetrator who came into possession of this terminal listing would need only the secret keyword to gain complete access to samplefile. The terminal user types in a three-digit keyword over the underscored characters.

(31) The keyword typed by the user does not match the authorized keyword and the computer indicates this.

(32) Because the terminal user did not pass the data security checks required to alter samplefile, the computer did not execute his request to have the 12-line file rewritten onto the original file; the original is preserved intact.

Retrieval from File (33-37)

Once again the user clears his file from the main memory of the CPU and lists a copy of the original file.

(33) The terminal user accesses the original file name "samplefile" on disk volume SRI 001.

(34) However, the user has not told the computer what to do with the 12-line samplefile he created in (20)-(25). Therefore, the computer asks the user to respond by typing "YES" if he wants the 12-line version of samplefile cleared from the main memory.

(35) The user responds affirmatively.

(36) The question mark indicates the previous command has been executed and the computer awaits another command. The terminal user responds by commanding the computer to list samplefile as it appears on disk.

(37) The computer lists samplefile. This listing is identical to the first listing (22); the data security features incorporated within samplefile protected it from modification by an unauthorized person.

Log-Off (38-41)

In this short series of interactions, the user completes his session on the time-sharing system and then receives a summary of accounting data.

(38) The user commands the computer to terminate his session and to erase the data he had called into the main memory of the CPU to work on. This will leave samplefile intact in its original form on disk.

(39) The computer acknowledges that a log-off has been executed by presenting the log-off date, day of week, and time of day.

(40) The computer presents the cumulative charge of the session.

(41) The computer indicates the session is over, and the log-off is complete.

Example 2

Table H-2 is another example of services available. The terminal interaction is provided. A line-by-line description of the exhibit follows.

The characters typed by the terminal user are those that are preceded by the greater than symbol (>). An exception to using this symbol is the user's password.

Equipment Authorization (01-02)

The terminal user has established a telephone communication link with the time-sharing service by dialing the correct telephone number. In the next two interactions, the user identifies his terminal type, and the computer system identifies itself to the user.

Table H-2

TIME SHARING LISTING: EXAMPLE 2

LINE REFERENCE	TERMINAL LISTING	
(01)	□	EQUIPMENT IDENTIFICATION
(02)	ONLINE - SUNY	
(03)	>L SUNY WPETRO	LOG-ON AUTHORIZATION
(04)	PASSWORD:	
(05)		
(06)	PASSWORD INCORRECT.	
(07)	PASSWORD:	
(08)		
(09)	PASSWORD INCORRECT.	
(10)	LOGGED OFF AT 11:48:08 ON 30MAY79	
(11)	□	EQUIPMENT IDENTIFICATION
	ONLINE - SUNY	LOG-ON AUTHORIZATION
(12)	>L SUNY WPETRO	
	PASSWORD:	
	PASSWORD INCORRECT.	
(13)	PASSWORD:	
(14)	A/C INFO:	
(15)	>RWH-TEST	
(16)	** ALL CLEVELAND USERS PLZ. TYPE 'INFO CLEMOVE' **	
(17)	SUNY READY AT 11.49.36 ON 30MAY79	
(18)	.302 10MAY78	RETRIEVAL FROM FILE
(19)	11.49.43 >L * NOMAD	
(20)	FILENAME FILETYPE MODE ITEMS	
(21)	THMMAN1 NOMAD P 20	
	THMMAN2 NOMAD P 21	
	THMMAN3 NOMAD P 68	
	THMMAN NOMAD P 20	
	THMMAN4 NOMAD P 110	
	EXP1 NOMAD P 12	
(22)	BAL NOMAD P 8	
	BAL1 NOMAD P 6	
	ART6 NOMAD P 8	
	ART4 NOMAD P 8	
(23)	11.50.22 >E BAL NOMAD	
(24)	EDIT:	
(25)	>P 40	
(26)	QUERY T;	
	SELECT PRODCD AMONG(350,580,690);	
	SELECT ADD REGNCD='WE' CAPYY=79;	
	CREATE BY COUNNM	
	BY COMPNM	
	BY LOCNM	
	ACROSS PRODSN AS A5 SUM(CAPTOT) HEADASIS ON T;	
	QUERY T;	
(27)	EOF:	
(28)	>TOP	
(29)	>LOC /BY/	
(30)	CREATE BY COUNNM	
(31)	>C /BY/QQQ/	
(32)	CREATE QQQ COUNNM	
(33)	>Q	

Table H-2 (Concluded)

LINE REFERENCE	TERMINAL LISTING	
(34)	11.51.32 >ATT PETRO	DATA SECURITY
(35)	PASSWORD:	
(36)		
(37)	PETRO ATTACHED AS T-DISK	
(38)	THE DATABASE IS CURRENTLY BEING UPDATED WITH NEW DATA. THIS PROCESS SHOULD BE FINISHED BY 30MAY79. FOR INFORMATION CONCERNING THE ITEMS BEING UPDATED, CONTACT SRI INTERNATIONAL. 29MARY79 RCH	
(39)	11.51.43 >LOG	LOG-OFF
(40)	3.02 ARU'S, .05 CONNECT HRS	
(41)	LOGGED OFF AT 11.52.03 ON 30MAY79	
	XO-	

(01) The user types a quad symbol (square), which is the character speed code that corresponds to the type of terminal he is using. The code may be obtained from the vendor. It allows the computer to translate messages to suit the terminal's speed and formatting characteristics.

(02) The computer indicates that it recognizes the user's terminal when it identifies itself as "ONLINE-SUNY," which means the user has established communication with a computer system in Sunnyvale, California.

Log-On Authorization (03-10)

In this series of interactions, the user must supply an authorized password before he may access computer files and use computer resources.

(03) The "greater than" sign is the computer's prompt to the user. The command typed by the user means he wishes to link into the computer system signified by the four-digit code "SUNY." "WPETRO" is the user's (1-8 digit) identification code. Note that this code is not concealed by underscoring.

(04) The computer prompts the user for his password.

(05) The computer prints the characters 8, M, and * on top of one another, on eight successive spaces to form underscoring. The user types his one- to eight-digit password over the underscoring. The presence of the underscoring prevents a potential perpetrator from obtaining the terminal user's password by viewing the computer listing.

(06) The password typed by the user in (05) did not match the authorized password that corresponds to the user name "WPETRO." The computer indicates this.

(07) The computer gives the terminal user a second chance to type the correct password. The user has 28 seconds to type the correct password.

(08) The computer types the underscoring over which the user types the password.

(09) Once again the user typed an incorrect password and the computer indicates this.

(10) If the user fails to type in the correct password on the second attempt, it is assumed that the user does not know the password, and the system is programmed to automatically log-off. The time and date of log-off are listed.

Equipment Identification (11)

Failure to type the correct password the second time requires the following procedure to be initiated.

(11) Following the automatic log-off, the user reestablishes telephone communication with the service and repeats the equipment identification steps (01-02).

Log-On Authorization (12-18)

(12) Once again, the user types in an invalid password and the computer indicates this. After the user has identified his terminal type and has been greeted by the computer system (11), he repeats the log-on authorization routine that he failed previously (03-10).

(13) The user is given a second chance to type the correct password.

(14) The computer prompt "A/C INFO" indicates the terminal user has typed in the correct password, and he should now type in a title or description of his computer run, which will appear on his computerized bill.

(15) The user responds by typing "RWH-TEST." "RWH" are probably his initials, and the word test will remind him when he reads his bill that this was a test run he made.

(16) The computer then printed a systems message that was initiated earlier by the computer operator and that automatically greets each user after the user has successfully logged on. This message probably was in regard to the move by the Cleveland office to a new facility.

(17) The computer's next message means the user has successfully gained access to the Sunnyvale computer system, which is ready to execute his commands. The time and date of access are given.

(18) The computer lists the name of the operating system being used— version 302—and the date it was placed in operation.

Retrieval from File (19-33)

In this sequence, the terminal user retrieves a file from a disk in permanent storage and edits the file copy while it is temporarily held in the main storage of the CPU.

(19) The computer lists the time and a greater than sign; this indicates the user has full access to the computer, and the computer awaits his first command. The terminal user responds by requesting the computer to list the directory of all his files written in the language called "NOMAD."

(20) The computer first prints the directory heading. "Filename" is the unique name that the user gives to each set of records he establishes. "Filetype" is the language and format type that characterize the file: other files may be a filetype, such as COBOL. "Mode" is the specific area that belongs to the user and where the file may be found: "P" refers to permanent storage. "Items" are the number of lines in the file. The directory is a preprogrammed feature of the operating system; it automatically updates itself whenever the user establishes or alters a file.

(21) These lines contain the listing of the user's files. The first listing is a file named "THMMANI" or "NOMAD" type, stored in the permanent section of the user's disk and consisting of 20 lines.

(22) The file named "BAL" is retrieved by the user in (23).

(23) The user presses the carriage return key of his terminal to indicate he is finished viewing his directory of files. The computer responds by printing the time and prompts the user for another command. The user commands the computer to edit the file named "BAL" of type "NOMAD" (22). Each file must be identified by its name and type, as the user has done.

(24) The computer acknowledges the command and prompts the user for specific editing instructions. The acknowledgment indicates the "BAL" file has been copied from the permanent section of disk to the main storage of the CPU. The file now resides in both permanent (disk) and temporary (core) storage.

(25) The user tells the computer to list (print) the first 40 lines of the file.

(26) The computer lists "BAL."

(27) "EOF" stands for end of file and means the entire file has been listed. The computer awaits further editing instructions. The computer listed 8 lines, although the user requested that the first 40 lines of "BAL" be listed. However, as may be seen (22), the "BAL" file only contained 8 items, all of which were listed by the computer.

(28) The user responds to the computer's prompt by commanding that the computer's "pointer" go to the top or first line of the file.

(29) The user then commands the computer to search the entire file and locate the word "BY."

(30) The computer lists the line in which the word "BY" is situated, signifying it has located the word and also giving the user a chance to verify that the computer has located the correct listing of "BY" if it happens to occur more than once in the file.

(31) The user commands the computer to change "BY" to "QQQ."

(32) The computer does this and prints out the modified line for user verification.

(33) The computer requests another command, and the user instructs the computer to "quit." This command deletes the copy of "BAL" in the main storage of CPU. It does not affect the original "BAL" file on disk, which remains unmodified. Had the user typed the word "file," the edited copy of "BAL" would have replaced the original copy on disk. The quit command deletes the altered version of the file held in temporary storage (main storage).

Data Security (34-38)

In this sequence, the user requests that a disk belonging to another user be attached. To access this protected disk, the terminal user must know and type the other user's password.

(34) Having quit his edit routine, the user is returned to command level communication with the computer, and the time is given. Prompted by the computer, the user commands that the disk belonging to a user code named "PETRO" be attached.

(35) The computer requests the password that corresponds to "PETRO." This data security measure prevents unauthorized users from viewing, modifying, or deleting data held in protected disk files.

(36) The user types the appropriate password over the underscored characters.

(37) The computer's message indicates that the password used was correct and that "PETRO" has been attached as the "T-DISK"; an arbitrary letter T is assigned as a title to "PETRO" to differentiate it from a "P" mode disk, which is the user's permanent disk.

(38) The originator of the disk preprogrammed this message to greet users who access his disk.

Log-Off (39-41)

In this sequence of interactions, the user terminates his communication with the computer, and the computer presents basic accounting information.

(39) The computer awaits the user's instructions about what to do with "PETRO." The user directs the computer to terminate his session at the terminal by typing LOG.

(40) The computer prints out accounting data. "ARU's" is an accounting algorithm that lumps CPU and I/O time into one unit figure. Connect hours are listed in hundredths of an hour.

(41) The computer lists that a log-off has been effected and the time and date it has been completed. The stray characters "XO-" are printed after the terminal link has been severed and therefore are not meaningful.

Example 3

Finally, a third example of popular time-sharing services is provided in Table H-3, followed by an explanation.

Following the log-on sequence, user commands may usually be identified as those characters preceded by a greater than sign (>).

Equipment Identification (01-02)

By dialing a phone number given to him by the vendor, the user establishes a telecommunication link with the time-sharing service; a high-pitched tone on the receiver is evidence of his contact with the service. After plugging the receiver into his computer terminal or communication modem, the user must identify to the computer network the type of terminal he is using. Correct identification of his terminal type will ensure that no characters are lost in his communication with the computer.

(01) The user presses the carriage return key and is prompted for his terminal identifier code. The prompt indicates he has a positive connection with the computer. The user types the code on the same line as the computer prompt. In this case, the user typed an "E," a code which means that the terminal used has a speed of 30 characters per second. The "E," however, does not appear on the listing.

(02) The computer responds by assigning a location code, "1017," Palo Alto, CA, and a port of entry number, "04," to the communication link. The code aids the vendor's staff in identifying specific user "links" in the event of communication problems.

Log-On Authorization (03-05)

In this series of interactions, the user must correctly identify himself to the computer system to be allowed access to data and computer resources. This step is the primary computer security defense against unauthorized users.

(03) The computer prompts the user for his user name, which may be from 1 to 8 digits. The user name serves to identify the storage space on the primary disk, which belongs to the terminal user. However, before the user is automatically linked to the storage space corresponding to the user name he typed, he must verify that he is authorized to access the data stored there. The password serves as the verification key. After the user types in his user name (03), he must type the password that corresponds with the user name he typed. The user types his password on the same line as his user name: the password does not appear on the thermal paper on which this dialog appears.

(04) The user typed an incorrect password in (03), and the computer indicates this. The computer again prompts the user to type his password.

(05) The log-on security system is designed to prompt the user for his password repeatedly for 2 minutes following the user's first connection with the system (01). If the user fails to type in the correct password during the 2-minute interval, he is advised to contact his vendor representative, and his telecommunication linked with the computer is automatically broken. This serves to deter unauthorized users from attempting to impersonate a user by guessing the user's password through trial and error.

Equipment Identification (06)

Failure to type the correct password in the 2-minute period necessitates initiation of the following procedure.

(06) The user must repeat the equipment identification steps (01 and 02) to reestablish a communication link with the computer. After establishing this link, he types in his user name and password as in (03).

Log-On Authorization (07-12)

(07) The computer's response indicates the user has typed in a correct password and is now in contact with the computer he wishes to use. The computer prompts the user to type in a project code, which is the session name that will appear on the user's bill. The system does not check for a valid project code. However, the user is given a limited

Table H-3

TIME SHARING LISTING: EXAMPLE 3

LINE REFERENCE	TERMINAL LISTING	
(01)	Please Type Your Terminal Identifier	EQUIPMENT IDENTIFICATION
(02)	-1017-04--	
(03)	Please Log In: DIST10E:	LOG-ON AUTHORIZATION
(04)	Error, Type Password:	
	Error, Type Password:	
	Error, Type Password:	
(05)	Please See Your Representative	
	If You Are Having Trouble Logging In	
(06)	Please Type Your Terminal Identifier	EQUIPMENT IDENTIFICATION
	-1017-04--	
	Please Log In: DIST10E:	LOG-ON AUTHORIZATION
(07)	Project Code:.LOGOFF AT 11:19:36 PDT TUESDAY 06/19/79 BY SYSTEM	
(08)	Please Log In: DIST10E:	
(09)	Project Code:Timeshare	
(10)	Logon At 11:20:10 PDT Tuesday 06/19/79	
(11)	CMS: R5.P02.Y29B 04/09/79	
(12)	** Notice ** CMS Field Test System	
	R;	DATA SECURITY
(13)	CMS	
(14)	C>ATT Filist	
(15)	Enter Read Password:	
	Filist As B/A-Disk	
	R;	RETRIEVAL FROM FILE
(16)	C>LI * * A	
(17)	ADDSDELS FOCEXEC B1	
	ALLABELS EXEC B1	
	ALLABELS FOCEXEC B1	
	BATCH1 EXEC B1	
	BATCH2 EXEC B1	
	CHANGES FOCEXEC B1	
	CLEAN EXEC B1	
	ET FOCEXEC B1	
(18)	??>KX	
	CMS	
(19)	C>T \ T\EDIT ADDSDELS FOCEXEC B	
(20)	E>T*	
(21)	TOF:	
	-START	
(22)	-Prompt &1.A1. Are There Any Additions To The Maillist Master File? Y or N.	
	-If &1 IS 'Y' GOTO ADD;	
	-If &1 IS 'N' GOTO NEXT;	
	Modify File Maillist	
	Prompt MC FT	
	Match MC	
	On Match Continue	
	On Nomatch Reject	
	Exit	
(23)	EOF:	
(24)	E>TOP	
(25)	TOF:	
(26)	E>L/PROMPT	
(27)	-Prompt &1.A1. Are There Any Additions To The Maillist Master File? Y or N.	

Table H-3 (Concluded)

LINE REFERENCE	TERMINAL LISTING
(28)	E>C/Y/Yes
(29)	-Prompt &1.A1. Are There Anyes Additions To The Mailist Master File? Y or N.
(30)	E>C/Yes/Y
(31)	-Prompt &1.A1. Are There Any Additions To The Mailist Master File? Y or N.
(32)	E>C/Y or N/Yes or No
(33)	-Prompt &1.A1. Are There Any Additions To The Mailist Master File? Yes or No.
	DATA SECURITY
(34)	FILE
(35)	SET NEW FILEMODE AND RETRY
(36)	QUIT
	LOG-OFF
(37)	R;
(38)	LOG
(39)	CONNECT= 00:06:52 TRU=
(40)	LOGOFF AT 11:27:02 PDT TUESDAY 06/19/79
(41)	Please Log In:

amount of time to type in either a project code or a carriage return, after which the computer will log him off the system. This security feature deters unknowledgeable, unauthorized users. The user did not type a project code or carriage return within the time given, and the computer executed a log-off, at the time specified on the listing.

(08) In logging the user off the system, the computer did not break the user's communication link. However, to access the system, the user must once again go through the log-on authorization process, as in (03-04). The user responds to the computer prompt by typing his user name and his password; the password does not appear on the listing.

(09) The user has typed a correct password and is prompted for his project code; he types "Timeshare," an arbitrary title.

(10) The computer responds by indicating that an authorized "LOG-ON" has been effected and gives the time and date of the log-on.

(11) The computer then identifies the operating system "CMS" with a code that details the version of CMS in use and when it was last modified; CMS is the abbreviation for CONVERSATION MONITORING SYSTEM.

(12) The version of the operating system with which the user is communicating is a field test version—which means it is still being tested and has not been completely debugged yet. Field test versions are usually used only by in-house personnel at the time-sharing service.

Data Security (13-15)

The data security precautions in the system ensure that files belonging to a user are accessed only by those persons authorized to do so by the originator of the file. Passwords are the primary security safeguard.

(13) After the log-on and system messages, the computer indicates it is ready by typing "R;".

(14) The CMS system indicates it awaits a command from the user with the prompt "C>". In response to the CMS prompt, the user commands CMS to attach the disk with the storage space on it that corresponds to the user name "PILIST".

(15) Before the user can access the "PILIST" files, he must pass a data security check; he must know and type the "read" password that corresponds to the user name "PILIST". Generally, the read password is not the same password as the log-on password. The read password is given out by the originator of "PILIST" to persons he allows to read the contents of his files; the user may not modify the file in any way. In response to the CMS prompt, the user types the "READ PASSWORD" for "PILIST"; the password does not appear on the listing. An acknowledgment follows successful entry of the read password.

Retrieval from File (16-33)

In this series of interactions, the user retrieves data from a file and attempts to modify the data.

(16) The user entered the correct read password in (15). In response to CMS's ready signal and its prompt for a command, the user types "LI**A," which tells CMS to list the names and types of all files on disk "A" that correspond to the user name "PILIST". The code "LB1" is a file security code that indicates a file has been established in a read-and-run mode and cannot be modified.

(17) The computer responds to the command in (16) by typing out an alphabetical directory of files belonging to "PILIST". "ADDSDELS" is the name of one of PILIST's files; its file type is "FOCEXEC"—a language type; its security mode is "B1," which cannot be modified, but can be read if the correct read password is given by the user.

(18) The user stopped the computer from typing the entire directory of "PILIST" files by typing "KX"—the escape key combination. The user had probably already identified the file information he had been searching for.

(19) CMS prompts the user for another command. The user mistypes a "T" and erases it. This is indicated by the "T". The user then tells the computer he wishes to edit or modify the file "ADDSDELS FOCEXEC B"

(20) The computer responds by switching from the CMS language to a text editing language. This is indicated by prompt "E>"; the CMS language prompted the user by typing "C>", in line (14). The user commands the text editor to list all the contents of the file by typing "T*"

(21) The text editor complies and begins with the notation "TOF:"—top of file.

(22) The text editor then lists the contents of the file as commanded.

(23) After the file has been listed in its entirety, the text editor system indicates this with the notation "EOF:"—end of file.

(24) The text editor prompts the user for another command. The user instructs the editor to go to the top of the file.

(25) The text editor indicates its "pointer" is at the top of the file.

(26) Prompted by the text editor, the user instructs it to locate and type the first sentence in the file with the word "PROMPT" in it.

(27) The text editor scans the sentences for the word prompt. It finds the word in sentence (22) and types out the sentence for user verification.

(28) The user responds to the text editor prompt by commanding it to change the first "Y" it finds in the sentence (22) to "Yes".

(29) The text editor follows the command precisely and prints the modified sentence for user verification: the first "Y" it located was in the word "ANY"; as per its instructions, it substituted the "Y" for "YES" leaving "ANYES" in place of "ANY".

(30) In reviewing the modified sentence (29), the user realized that the word "ANY" had been modified instead of the letter "Y" at the end of the sentence as had been his intention. He instructs the text editor to undo his previous modification.

(31) The text editor implements the user's instructions and types the modified sentence for user verification.

(32) The user responds to the text editor's prompt by instructing it to replace the phrase "Y or N" with the phrase "YES OR NO", so as to avoid the problem he encountered in (28) and (29).

(33) The text editor implements this instruction and lists the modified sentence for user verification. The user notes that his intentions have been fulfilled; by switching the single character "Y" or "N" response choice to a multicharacter "YES" or "NO" response choice, he has modified the program in a way that will prevent it from running correctly.

Data Security (34-36)

The following steps are in response to the text editor's request for another command.

(34) The user instructs the text editor to file onto disk the revised copy of "ADDSDELS" in place of the original.

(35) The text editor does not implement the user's command because "ADDSDELS" is a file of mode B; it can be read by persons who know the read password, but it can only be modified by the originator of the file. The text editor instructs the user to modify the "FILEMODE" of "ADDSDELS" or to have the originator of the file modify it to allow the user to edit contents of the file.

(36) The text editor prompts the user for another command. Because the user is unable to insert the revised file into permanent disk storage, perhaps because his change was an unauthorized one, he instructs the editor that he wishes to cease his attempt at editing "ADDSDELS", and wants his revised copy deleted from the main storage of the CPU; the original file is left unchanged.

Log-Off (37-41)

In this series of interactions, the user completes his session, instructing the computer to log him off, and basic accounting data are listed by the computer.

(37) The CMS system is now ready. The user is no longer communicating with the text editor.

(38) CMS requests a command. The user instructs it to log-off by typing "LOG".

(39) The computer types accounting details for the session just completed. "CONNECT" is the amount of time the user was in communication with the time-sharing service. "TRU" is the vendor's resource use algorithm, which combines I/O, CPU time, paging, and other services into one unit. Finally, the project code is listed.

(40) The computer notes that a log-off has been completed and gives the time and date it was effected.

(41) The computer awaits the next time-sharing session, requesting that the user sign-on.

APPENDIX I

Directories and Databases for Contacting Expert Witnesses

APPENDIX I: Directories and Databases for Contacting Expert Witnesses

Consultants and Consulting Organizations Directory, Gale Research Co, Book Tower, Department 77748, Detroit, MI 48277-0748; (313) 961-2242, (800) 223-4253.

Directory, Information Systems Security Association (ISSA), P.O. Box 9457, Newport Beach, CA 92658; (714) 250-4772, Richard V. Rueb, Executive Director.

Directory, International Association of Professional Security Consultants, 835 Deltona Blvd., Suite 77, Deltona, FL 32725; (904) 789-7878, Steven R. Keller, CPP, Executive Director.

Directory, Professional and Technical Consultants Association, 1330 Bascom Ave., Suite D, San Jose, CA 95128-4502; (408) 287-8703, Georgiana Shepherd, Executive Director.

Directory of Consultants in Computer Systems, Gale Research Co, Book Tower, Department 77748, Detroit, MI 48277-0748; (313) 961-2242, (800) 223-4253.

Directory of Experts and Consultants in Science and Engineering, Research Publications, 900 Armour Drive, Lake Bluff, IL 60044; (312) 234-1220.

Expert Witness Network, Consultation Networks Incorporated, 1608 New Hampshire Ave., NW, Suite G-100, Washington, D. C., 20009; (202) 667-6961, (800) 345-5993; Gary Melickian and George S. Jenkins.

Forensic Services Directory, National Forensic Center, 17 Temple Terrace, Lawrenceville, NJ 08648; (609) 883-0550, (800) 526-5177; Betty Lipscher, Director.

The Lawyers' Desk Reference (Contains Directory of Specialists Section), 2920 E. Jefferson, Detroit, MI 48207; (313) 259-7200; J. R. Philo, Editor.

Nationwide Expert Witness Directory, Nova Law Publications, Inc., P.O. Box 17975, 5625 Turkey Road, Pensacola, FL 32522; (904) 455-2221, 1-(800) USA-XPERT, Larry W. Vallia, Publisher, Editor in Chief.

Technical Advisory Service for Attorneys (TASA), Technical Advisory Service, Inc., 428 Pennsylvania Avenue, Fort Washington, PA 19034-3479; (215) 643-5252, (800) 523-2319; Carol G. Stein, Manager.

Who's Who in Technology, Gale Research Co, Book Tower, Department 77748, Detroit, MI 48277-0748; (313) 961-2242, (800) 223-4253.

Index

4GLs, 120
Access, 84, 86, 87, 100, 134
  devices, 100
Accountant, 19
ACF2, 134
ADA, 112
Admissible, 66, 74, 76-78
Admission, 77, 78
Agriculture, Department of, 109
Airline reservation systems, 55
Alias, 20
Alter, 88
American Bar Association, 5
American Law Reports, 63
Analog, 131
Antagonistic personnel, 40
Antitrust, 78
  violations, 7
Antivirus computer programs, 16
APL, 120
Apple IIe, 68
Application, 130
  programmer, 13
APT, 120
Arithmetic, 116
Arizona, 83, 88
Arson within Special Maritime and Territorial Jurisdiction, 107
Artificial intelligence, 64
ASCII, 113
Assembler, 119
Asynchronous, 20, 131
  attack, 22
AT&T, 132
ATM, 135
Atomic Energy Commission, 106
Audett vs. United States, 107
Audit, 67, 68, 70
  log, 22, 30, 123
  organization, 35
  trail, 20, 29, 30, 58
Auditor, 19, 28, 30, 33, 63, 134
Authentication, 10, 74
Automated teller machine, 9, 84, 86, 135
Automatic callback devices, 12
Availability, 3, 9

Backup, 15, 17, 32, 48, 50, 56, 58, 70
Background check, 40
Bank Administration Institute, 34
Banking system, 18
BASIC, 112
Batch, 124, 129
Batch control totals, 12
Bernhardt vs. United States, 10
Best evidence rule, 74, 80
Bit-mapped, 71
Blachly vs. United States, 105
Block mode command, 15
Boot, 17, 72
Breach of contract, 78
Bribery, 7, 38
British Broadcasting System, 6
Browsing, 89
Brunette vs. United States, 108
Bugging, 93
Bugs, 80
Burglary, 24, 58, 86, 106
Burnett vs. United States, 102, 105
Business crime, 2
Business records, 27

C, 112
California, 84, 88, 93, 96
  Evidence Code, 67
Carbon paper, 14
CBS (TV), 6
Certified public accountant, 36
Chaos Computer Club, 4
Check, 92
Check sum, 15, 17
Checkpoint restart, 22
Civil, 88, 94, 100
Classification, 3, 4
COBOL, 112
Collusion, 7, 12, 38-40
Colorado, 87
COM, 121
Commercial programs, 23
Commodore 64, 68
Common law, 7
Communication, 65, 85, 94, 97-99, 111, 130
  carriers, 132
  controller, 11
  service providers, 32
  technology, 111
Compilation evidence, 80
Compiler, 119
Computer
  abuse, 2, 9
  center, 13
  circuitry, 21

Computer *continued*
crime, 2
larceny, 24
listings, 14
manager, 13
manufacturer, 51
operations, 17, 47, 75
operator, 29, 40, 67, 70, 123
program, 21, 22
records, 76
reports, 68
scientists, 29
security specialists, 27, 28, 32
services, 32, 44
technology, 111
users, 30
virus, 16
Computer Fraud and Abuse Act, 83
Computer Fraud and Abuse Act of 1986, 84, 96
Computer Fraud and Abuse Act of 1987, 5
Computer-related crime, 2
Concealing, 101
Confidentiality, 3, 9, 71, 73, 109, 129
Congress, 7, 84, 96
Congressional Subcommittee on Crime, 7
Console, 66, 70
Console logs, 29, 72
Conspiracy, 78, 101, 108
Constants, 117
Consumers Union
vs. Veterans Administration, 109
Control bypass, 20
Conversion, 102
Copyright, 23, 32, 63, 75, 100
Corruption, 7
Counterfeit, 8, 12, 92, 100, 101, 104
Courtroom knowledge, 27
Court, 63, 73, 74, 76-81, 86, 88, 92, 99
testimony, 27
demeanor, 27
cross examination, 27
CPU, 122
Crackers, 40
Credit, 84
Credit Card Fraud Act of 1984, 96, 99
Credit card, 85, 89, 91, 100, 128
number, 10
Credit union, 44
Criminal enterprise, 25
Criminal justice agency, 72
Criminal justice community, 5
Cross-examination, 27
Cryptography, 9, 106
Customer file, 115
Customer record, 115
Damage, 87, 88, 94, 96, 99
Data, 85, 89
backup, 32
base, 114, 128
base management system, 31, 56, 115, 128
communications, 55-57, 67, 130
Encryption Standard, 135
entry, 29, 39
leakage, 23
security specialist, 32
switch pass-through, 12
DBMS, 31, 115, 120, 128
Deal vs. United States, 107
Debit instrument, 101
Debugging, 20
Deceptive Practices, 107
Decision, 117
DECNET, 132
Defense, 106
Definition of computer, 64
Definition of computer crime, 2
Delaware, 85
Demon programs, 10
Deputy district attorneys (DDAs), 6
DES, 135
Desk-top publishing, 31
Destroy, 88, 90, 96, 97, 99
Destruction, 94
Dialed number recorder (DNR), 10, 68
Differential association, 39
Digital, 131
Direct access, 126
Disclosure, 109
Discovery, 79
Disk sector, 17
Diskette, 17, 24, 67
District of Columbia, 93
Drug Enforcement Administration, 77
Duplication, 89, 91

E-mail (see – Electronic mail)
Eavesdropping and spying, 9
EBCDIC, 113
Editing, 117
EDP audit, 27, 33, 63, 67
tools, 34, 35
auditor, 34
Edwards vs. United States, 108
EFTs, 91, 134
Electronic access, 10
Electronic bulletin board, 68, 97
Electronic Communications Privacy Act (ECPA), 9, 83, 96, 97
Electronic data interchange, 1, 73, 134
Electronic door access, 12
Electronic Fund Transfer Act, 101

Electronic fund transfer, 91
Electronic letter bomb attack, 15
Electronic mail, 14, 32
Embezzlement, 38, 101, 103, 105
Encryption, 11, 68, 71, 98, 135
Engineering, 55, 127
Engineers, 30, 43
English, 65, 75, 115
Erase, 14
Espionage, 31, 32, 61, 94
Espionage Act, 9
Ethernet, 134
Evidence, 63, 66-68, 71-74, 76-78, 85, 86
  compilation, 80
Exclusionary rule, 66
Expert, 27, 63, 66, 74, 76, 78, 79
Extortion, 60

Facilities management company, 31
False data entry (data diddling), 12, 20, 29
Faraday, 61
Faraday-cage, 9
FAX, 129
FBI, 78, 96, 97
  Academy, 5
Federal Communications Commission, 9, 98
Federal Copyright Act of 1976, 96, 100
Federal Criminal Code Provisions, 102
Federal Penal Laws, 96
Federal Privacy Act of 1974, 101
Federal Rules of Evidence, 27, 74
Fictional stories, 6
Fields, 114
File, 114, 123, 125, 128
File server, 17
Financial Institutions Regulatory and Interest Rate Control Act of 1978, 101
Financial instrument, 85
Fingerprint, 10, 68, 73
Firmware, 80
Florida, 84, 86
FOCUS, 120
Foreign governments, 104, 106
Forensics, 73
Forgery, 12, 89-92, 104, 105
FORTRAN, 21, 28, 112
Foundation requirements, 76
Foundational problems, 76
Fourth generation languages, 120
Fraud, 31, 33, 36, 38, 66, 68, 83, 86-88, 96, 101, 103-105
Frequency, 5
Funds, 68

Gathering, Transmitting, or Losing Defense Information, 106
General ledger, 25, 45
Geographic, 1
Georgia, 83
Gorin vs. United States, 106
GTE, 132

Hacker, 10, 24, 30, 40, 67, 68, 100
Hancock vs. Decker, 95
Hancock vs. State, 92, 94
Hand geometry, 10
Hard-wired cables, 11
Hash totals, 17
Haas vs. Henkel, 108
Hawaii, 84
Hearsay
  business record exception, 74
  evidence rules, 67
  exception, 76
  rule, 76, 77
History, 5
Horse, 15

I/O bound, 30
IBM, 113, 131, 135
IBM compatibles, 68
Idaho, 85
Immunity, 81
Impersonation, 58, 107
In camera, 73
Incarceration, 8
Income tax returns, 77
Indexes, 117
Informant, 66
Information Systems Security Association, 67
Information
  integrity, 9
  security, 33
  services, 45
Informers, 66
Input, 121, 124
Institute of Internal Auditors, 33, 67
Insurance fraud, 25
Integrity, 3, 63, 67, 71, 72, 75
Intelligent terminals, 133
Interception, 98
Interference, 94, 98
Internal Revenue Service, 5, 79
International Standards Organization, 132
Interstate Commerce, 103
Interstate transportation of stolen property, 103
Interviewing a suspect, 42
IRS (see — Internal Revenue Service)

Jackpotting, 10
Jargon, 1, 9, 80, 84
JCL, 123
Jerome vs. United States, 106

Job, 14, 29, 47, 48, 51, 72, 75, 77, 123
Journalist, 6
Judge, 81
Jurisdiction, 74, 89, 96
Jurisdictional, 86
Jury, 27, 73, 80
Justice Department, 97, 109
Justice System Administration Improvement Act, 7
Juvenile delinquents, 9

Kaplan, John, 95
Keyboard, 74
Keystroke rhythm, 10

LAN, 134
Language, 119, 123
Laptop computer, 57, 64
Larceny, 24, 58, 86, 89, 90, 92, 95, 96, 107
Leak data, 23
Legal definitions, 63
Legislation, 97
Legislative response, 83
Legislatures, 85
Lewis vs. United States, 107
Lexis, 31
Local, 126
Local area networks, 134
Log, 66, 67, 70-72, 78, 123, 128
Logic bomb, 15, 21, 23
Logic errors, 20
Logical, 117
Loops, 117
Los Angeles, 6

Magnetic card key, 11
Magnetic stripe card, 10
Mail fraud, 105
Mainframe computer, 27, 121, 123
Malicious Injury to Government Property, 108
Malicious mischief, 86
Management information system, 31
Mantrap, 11, 52
Manufacturing organizations, 32
Masquerading, 10
Massachusetts, 84
MCI, 132
Memo-posting, 129
Memory, 122
Metal key, 10, 11
MICR, 121
Microcomputers, 24, 30, 111, 121
Microwave, 9, 32
Minicomputers, 30, 121
Minors, 88
Misappropriation, 94
Missouri, 84
Modem, 11, 56
Morgan vs. United States, 105
Morissette vs. United States, 105
Multiprocessing, 124
Multiprogramming, 124

NASA, 4, 106
National College of District Attorneys, 5
National District Attorneys Association Economic Crime Project, 5
National security, 106
NBC TV News, 6
Network Operators, 29
Networks, 30, 32, 56, 54, 65, 85, 89, 111, 121, 132, 133
Nevada, 84
New Jersey, 93
New York, 89, 96
New York City, 6
New York Times Co. vs. United States, 106
News media, 6
News reporters, 6
Newspaper, 79
NOMAD, 120

O'Keiley vs. United States, 103
Object code, 17
OCR, 121
Oklahoma, 85
On-line, 126, 129
Open Systems Interconnect, 132
Operating system, 15, 17, 20, 22, 45, 65, 70-72, 122, 123
Operations reports, 50
Optical disks, 14, 122
Optical fibers, 32
Organizational issues, 7
Organized crimes, 25
Output, 121, 126

Packets, 132
Paper, 66, 79, 95, 100, 103
Paper company, 14
Parameters, 117
Parent, 88
Password, 10, 11, 20, 30, 52, 58, 97, 100, 134
Patent, 75
Payroll, 44, 45, 125
Pen register dialed-number recorder, 10, 11, 68, 99
Penalties, 85, 98
Pennsylvania, 93
People vs. Dolbeer, 95
People vs. Earle, 95
People vs. Glover, 90
People vs. Goetz, 90
People vs. Mackey, 90
Personal computer, 68, 111, 121

Personal computer users, 30
Pest, 16
Philadelphia, 6
Photographing and Skeiching Defense Installations, 106
Physical access, 10
Piggybacking, 10, 11
Piracy, 23, 94, 100
  pirated programs, 24
PL/1, 120
Playback, 10
Point-of-sale terminal, 29, 121
Polling, 127
Pollution, 7
POS terminal (see — Point-of-sale terminal)
Postal Inspection, 5
Postal Service, 105
Preliminary facts, 74
Price fixing, 7
Privacy, 73, 79, 96, 99, 101
Process control, 129
Processing, 125, 130
Production programs, 13, 15
Production Steps, 70
Professional associates, 27
Program, 21, 22, 115
Programmable calculator, 43
Programmer, 19
Property, 85
Proprietary rights, 75
Prosecution, 74
Protocol, 131
Punched card, 47, 49, 68, 73, 80

Quality control, 130
Questionnaire, 6

RACF, 134
Radiation, 9
Radio, 32
Radio frequency, 9, 61
Radio transmitters, 9
RAMIS, 120
Real-time, 68, 126
Reasonable particularity, 66
Records, 76, 114
Recovery, 128
Regional Bell Operating Companies, 132
Regulatory offenses, 8
Remote, 126, 133
  facility, 17
  job entry, 48
Report production, 71, 72
Residual data, 14
Restarts, 128
Retinal pattern, 10
Reuse, 14
Rhode Island, 85
Ribicoff, Sen. Abraham, 5
RJE (see - Remote)
Robin Hood Syndrome, 40
Root directory, 17
Round down fraud, 18
RPG, 120

Sabotage, 31, 32, 38, 50, 60
Safeguards, 52, 67, 73, 75
Salami attacks, 15, 18
Satellite communications, 9, 32
Scanning, 10, 23
Scavenging, 14
Scientific, 55
Scientists, 29, 30, 43, 127
Scrambling, 135
SDLC, 131
Search and seizure, 66, 73
Search warrant, 63, 66, 68
Secrecy, 63, 73, 75, 109
Secret Service, 5, 96, 97
Securities and Exchange Commission, 5
Security, 123, 129, 134
  consulting services, 27
  specialist, 27, 28, 32, 67
Self-learning, 64
Separation of responsibilities, 12
Sequence numbers, 12
Serialization, 20
Service bureau, 25, 27, 32, 39, 40, 75
Shoulder surfing, 9
Shrink-wrap, 23
Simulation, 25
Skills, 9, 15, 27, 39, 72
Smart card, 10
SNA, 131
Software, 65, 67, 80, 85, 88, 89, 97, 115
Source code, 17
Spooler, 133
Spread sheet applications, 65
SRI Computer Abuse Methods Model, 4
Stanford School of Law, 95
State penal laws, 83
State vs. Shultz, 93
State vs. Tonnisen, 93
Statistics, 5, 8
Steal, 102
Storage, 122
Subpoena, 99
Subroutines, 118
Superzapping, 13, 71
Suspects, 27, 36
SWIFT, 134
Switches, 118
Synchronous, 131

Systems analysis, 28, 30, 31, 46, 47
Systems programmer, 28

Tables, 118
Tailgating, 11
Tampering, 89, 90, 94, 108
Tandy TRS 80, 68
Tax evasion, 77
Tax fraud, 8
Taxonomy, 4
Telemarketing, 10
Telephone
  lines, 99
  numbers, 10
  switching, 11
Teleprocessing, 130, 132
Teletypes, 133
Terminal, 11, 52, 56, 58, 59, 68, 70, 76, 122, 123, 126, 128, 133
Testimony, 27
Texas, 14
Theft, 24, 76, 86, 87, 89, 91-93, 101, 103-105
Theft within Special Maritime and Territorial Jurisdiction, 105
Tillman vs. United States, 108
Time bomb, 17, 21
Time of preparation, 76
Time-sharing, 25, 55, 58, 68, 75, 76, 127
  services, 31
Timeliness, 86
Timing, 1
Token, 10, 11, 30
  ring network, 134
Top Secret, 134
Trade secret, 23, 32, 73, 75, 76, 84, 94, 95
Trafficking, 100
Trap doors, 20
Trash barrels, 14
Trespass, 83, 86, 88-90, 94, 106
Trial, 74, 78, 79, 111
Trier of facts, 74
Trojan horse, 15, 20, 21, 23, 71

Unauthorized, 87, 90, 105, 109
Unconstitutional, 86
Uniform Business Records as Evidence Act, 77, 78
United States ex. rel. Norwegian Nitrogen Products Co. vs. United States Tariff Commission, 109
United States vs. Achtenberg, 108
United States vs. Anderson, 102
Unifed States vs. Astolas, 103
United States vs. Ballard, 107
United States vs. Banks, 107
United States vs. Bottone, 102, 104
United States vs. Chase, 108
United States vs. Digilio, 102
United States vs. Donner, 108
United States vs. Drebin, 104
United States vs. Drummond, 106
United States vs. Eberhardt, 108
United States vs. Echevarria, 102
United States vs. Gardner, 102
United States vs. Giles, 107
United States vs. Greenwald, 104
United States vs. Handler, 104
United States vs. Hassel, 103
United States vs. Heine, 106
United States vs. Henry, 105
United States vs. Jacobs, 103
United States vs. Johnson, 109
United States vs. Jones, 104
United States vs. Lambert, 103
United States vs. Lepowitch, 107
United States vs. Lester, 103
United States vs. Maddox, 103
United States vs. Owens, 106
United States vs. Poindexter, 107
United States vs. Rogers, 106
United States vs. Roselli, 103
United States vs. Seidlitz, 104
United States vs. Sheridan, 103
United States vs. States, 105
United States vs. Tijerina, 102
United States vs. Tyers, 103
United States vs. Zavala, 105
United States
  attorneys, 8
  Congress, 85
  Criminal Code, 3
  Department of Agriculture, 109
  Department of Defense, 6, 106, 112
  Department of Justice, 96
  Department of Justice, Bureau of Justice Statistics, 6, 83
  National Bureau of Standards, 135
  Senate Government Affairs Committee, 5
  Supreme Court, 75
  Treasury, Federal Law Enforcement Training Center, 5
Universities, 27
UNIX, 20
Update-in-place, 129
User, 30, 31, 67, 72, 73, 75, 84, 87, 90, 97
User ID, 10, 30, 134
User-friendly, 8
Utility program, 13, 15, 70, 76, 77

Vandalism, 58, 60
Variables, 117
VDTs, 122, 126, 133
Video recording, 9
Virginia, 92, 94
Virus, 15, 16
Visual aids, 80

Voice, 10
Vulnerability, 27, 36, 39, 52, 57-60, 67, 72

W-2 federal income forms, 12
WANs, 134
Ward vs. California, 39, 75
Ward vs. Superior Court, 95
Weir vs. United States, 107
Weiss vs. United States, 105
Westlaw, 31
Whistle blowers, 89
White House, 14
White-collar crime, 2, 7, 25, 38, 39
  statistics, 8
Winer vs. United States, 103
Wire Fraud Act, 96, 100
Wiretap, 9, 10, 97
Witness, 27, 63, 68, 74, 76, 80
Workstation, 45, 55, 121
Worm attack, 16
Wyoming, 84

U.S. Department of Justice
National Institute of Justice

Washington, D.C. 20531

BULK RATE
POSTAGE & FEES PAID
DOJ/NIJ
Permit No. G-91

Official Business
Penalty for Private Use $300